

# User Guide

VFC 2.11.11.11

Copyright © 2005-2012 Michael A. Penhallurick MSc

All rights reserved.

The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by the author.

The author assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is furnished under license on a subscription basis and may only be used or copied in accordance with the terms of such license. Certain advanced program features will cease to function once the subscription period expires.

VMware® is a trademark of VMware, Inc. and may be registered in certain jurisdictions.

Microsoft® and Microsoft® Windows® are trademarks of Microsoft Corporation that may be registered in certain jurisdictions.

All other products or name brands are trademarks of their respective holders and are acknowledged.

VFC IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW THE AUTHOR WILL BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## Table of Contents

<a href="#">Overview.....</a>	<a href="#">4</a>
<a href="#">Installation of VFC and associated applications.....</a>	<a href="#">6</a>
<a href="#">Installation of VFC (VFC2-Setup.exe).....</a>	<a href="#">7</a>
<a href="#">The VFC Dongle and Dongle Drivers.....</a>	<a href="#">10</a>
<a href="#">The VFC License Manager.....</a>	<a href="#">14</a>
<a href="#">Installation of VMware Workstation.....</a>	<a href="#">16</a>
<a href="#">Installation of VMware VDDK.....</a>	<a href="#">22</a>
<a href="#">Installation of Mount Image Pro.....</a>	<a href="#">27</a>
<a href="#">Change Application Shortcuts to 'Always run as administrator'.....</a>	<a href="#">32</a>
<a href="#">VFC: Step-by-Step.....</a>	<a href="#">34</a>
<a href="#">Mount a forensic whole disk image.....</a>	<a href="#">34</a>
<a href="#">Select Source Device – Mounted Hard Disk.....</a>	<a href="#">36</a>
<a href="#">View Sectors.....</a>	<a href="#">38</a>
<a href="#">Select Partition.....</a>	<a href="#">39</a>
<a href="#">Password Bypass.....</a>	<a href="#">45</a>
<a href="#">VMware Tools Installation.....</a>	<a href="#">47</a>
<a href="#">System Restore.....</a>	<a href="#">49</a>
<a href="#">Creating a standalone Virtual Machine from a VFC VM.....</a>	<a href="#">56</a>
<a href="#">Standalone VFC VM using a DD image.....</a>	<a href="#">56</a>
<a href="#">Duplicate VFC VM using disk-copy method.....</a>	<a href="#">56</a>
<a href="#">Cannot open the disk.....</a>	<a href="#">76</a>
<a href="#">Host System is Windows 7 on a Boot Camp Mac Pro.....</a>	<a href="#">78</a>
<a href="#">Could Not Unload Registry.....</a>	<a href="#">79</a>
<a href="#">Frequently Asked Questions.....</a>	<a href="#">80</a>
<a href="#">The Creator of VFC.....</a>	<a href="#">84</a>

## Overview

VFC (Virtual Forensic Computing) is a forensic application designed to handle a variety of hard disk drive sources (physical disk, bit-for-bit disk copy or forensic image file) and successfully transpose over 95% of such images into virtual machines - without expensive physical hardware disk caches or time-consuming conversion processes.

VFC is designed to predominantly utilise user mounted forensic whole-disk image files which are then presented to the system as an available physical disk.

This mounted disk is read-only and cannot be directly modified.

VFC can also utilise (write-blocked) 'real' physical disks or bit-for-bit 'flat' disk images, commonly referred to as RAW or DD images.

Without the use of a write-block device, original disks can (and probably will) be altered, thus compromising the integrity of the original data. The same is true of DD images when accessed directly.

VFC interrogates the selected device and calculates the disk geometry and partition information. It uses these calculations to create a virtual disk cache so that the required partition can be queried without risk of altering the underlying data.

Once the image source has been selected, VFC will list the available partitions and display them on the main system dialog. In general, the partition marked 'Bootable' will be the one containing the Operating System. With certain systems (such as Windows Vista and above) the bootable partition may only be around 100MB and will not actually contain an OS. In these instances, select the next available partition, which will typically occupy the remainder of available disk space and will contain the OS.

Once the required partition is selected, VFC default behaviour is to analyse the OS by querying registry data and system files. The resultant information thus gleaned is displayed on the main VFC screen.

At this stage, VFC has sufficient information with which to create the required disk files and inject any required system fixes. The default file names of 'New Virtual Machine' and 'New Virtual Disk' can optionally be manually changed prior to generation of the VFC VM.

Once the VFC VM has been generated, the launch facility is enabled and the machine can be booted into a virtual environment. Whilst there may be some limitations (particularly with screen resolution and OEM hardware devices), the user can then interrogate and interact with the virtualised system in as close an approximation to the original as is possible.



If a logon password is required but not known, the machine can be suspended and the VFC Password Bypass routine can be utilised. (Windows Only)

If there are system restore points available, the in-built Windows System Restore feature can be used to 'rewind' the VFC VM to an earlier date. In so doing, this will undo necessary changes that the initial generation has implemented and the system will fail to boot from a restored session.

This is expected behaviour.

Simply power off the VFC VM and utilise the Restore Point Forensics feature to re-inject the necessary system drivers and thus enable a successful boot to the required System Restore Point.

## **Installation of VFC and associated applications**

VFC has been developed in order to automate and expedite the steps required to implement The VFC Method of creating a functional working VMware Virtual Machine (VM) (primarily) from a mounted Expert Witness Format (EWF) file.

As the above indicates, one of the required components of this methodology is access to and use of the VMware Virtualisation platform. The recommended platform is VMware Workstation, as this application provides additional functionality over other available VMware desktop platforms, which the end-user investigator may find useful. VFC can also create VMs that will work with VMware Player and VMware Server 2. The latter products are available for free (with registration) from VMware directly.

Another component required in order to successfully use VFC is the vmware-mount utility which is deployed within the VMware VDDK (Virtual Disk Development Kit, currently at v5.0). The vmware-mount utility is used to mount a specific volume of a virtual disk (via snapshot files) so that access can be gained to the file system in a forensically sound manner.

Whilst VFC is predominantly used with images mounted using GetData's Mount Image Pro (MIP), it is also capable of accessing images mounted with the Encase Physical Disk Emulator (PDE) or the AccessData FTK imager mounting utility. Other utilities may also be available but these have not been tested by the author.

NB: VFC utilises a mounted physical disk, a 'real' physical disk or a raw, bit-for-bit, 'dd' image.

The VFC Method and the VFC application have been wholly developed utilising MIP.

There have been mixed reports with using the FTK imager mount utility in that some images would not virtualise unless mounted with MIP.

When using the Encase PDE, the end-user is limited to mounting a single disk via the EnCase interface.

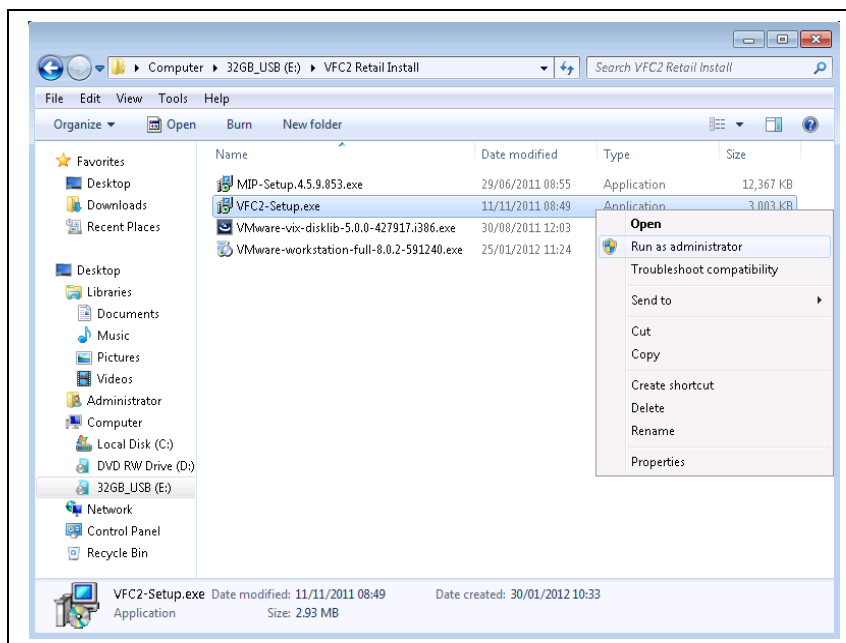
It has been found that the best method of installing VFC and other required applications when using a Windows 7 host system is by right clicking the relevant executable and selecting 'Run as Administrator' from the subsequently displayed context menu. It is the author's opinion that UAC can cause issue and should also be disabled on the forensic investigators host system; however this is a decision left entirely up to the investigator.

The host system used to create the following screenshots was an Intel based Mac Pro running Windows 7 Ultimate x64. Boot camp drivers were NOT installed.

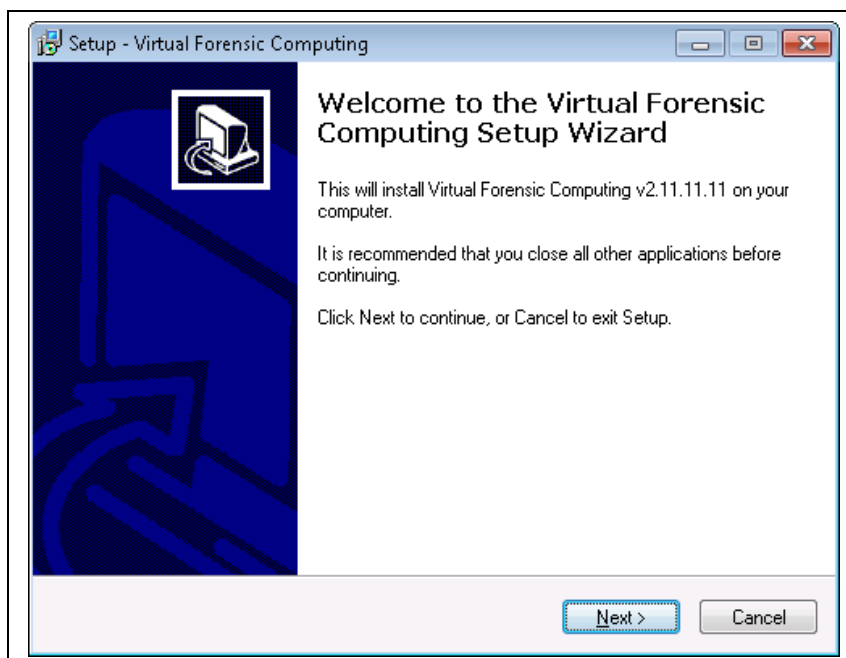
The following instructions relate to the installation of VFC 2.11.11.11, VMware Workstation 8.0.2; VDDK 5.0 and MIP 4.5.9.853.

The latest versions (or links to the latest versions) are available from:  
<http://www.md5.uk.com/products/vfc2/download-vfc>.

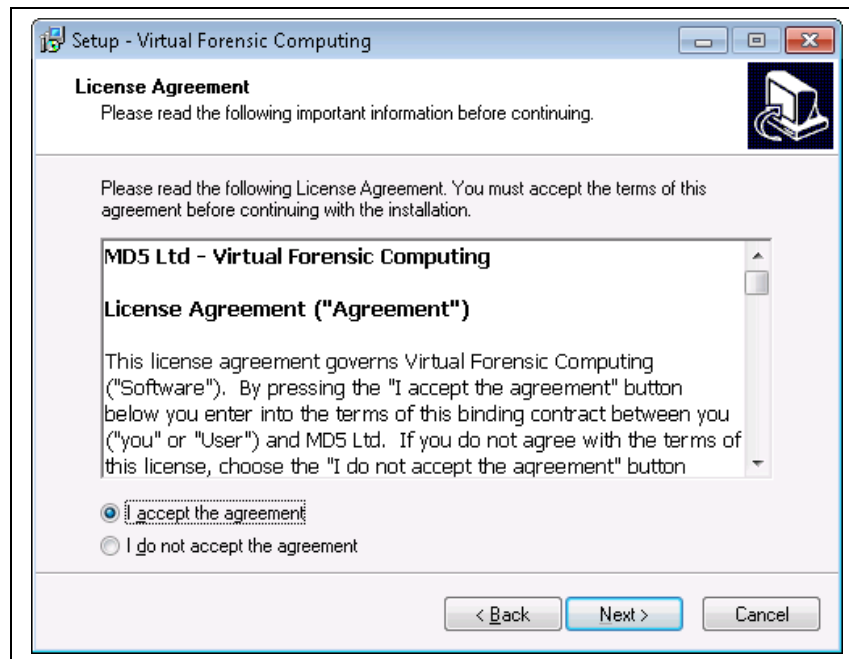
### *Installation of VFC (VFC2-Setup.exe)*



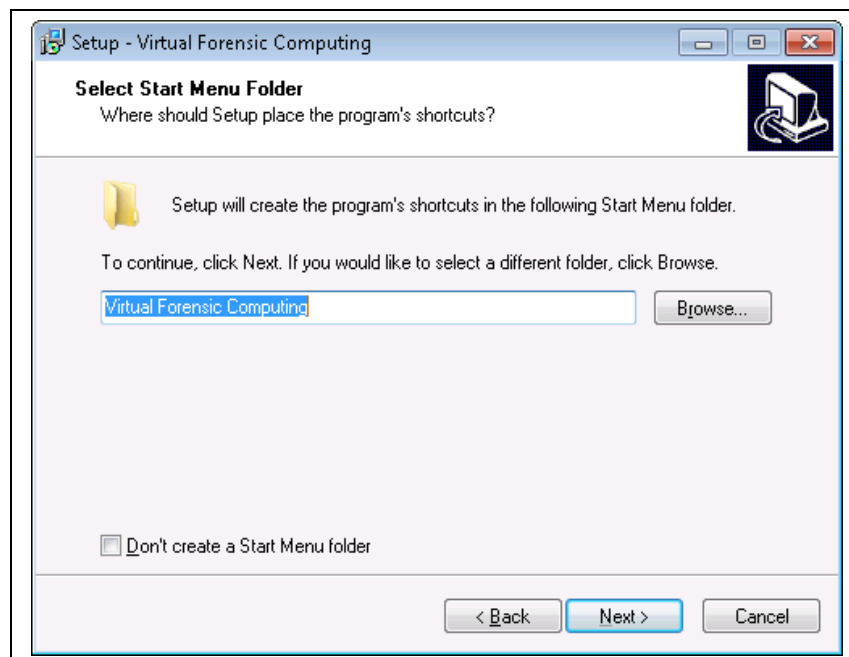
In Windows Explorer, navigate to the location where you have saved the installation files, right-click on the VFC2-Setup.exe file and select 'Run as administrator'.



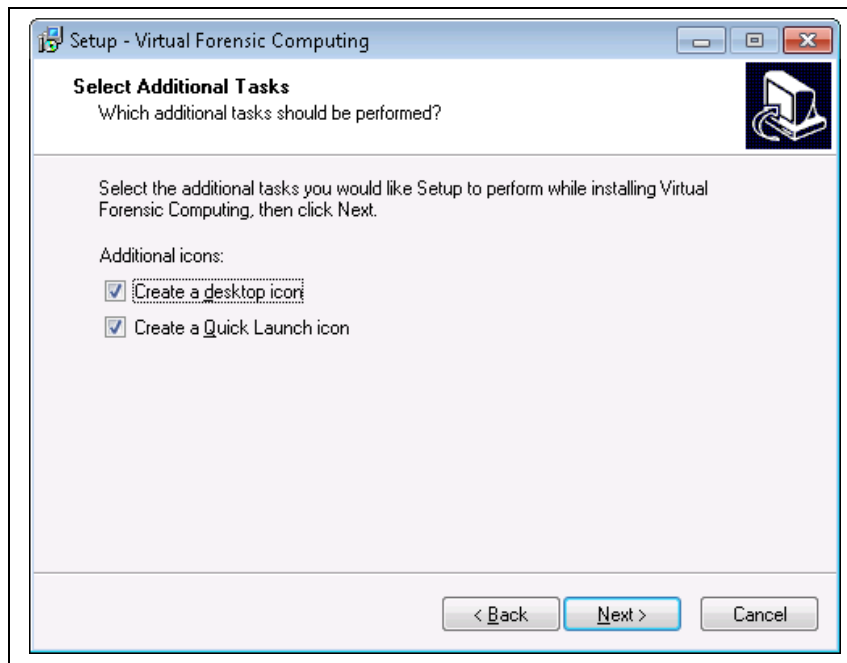
Click 'Next' and accept the End User License Agreement.



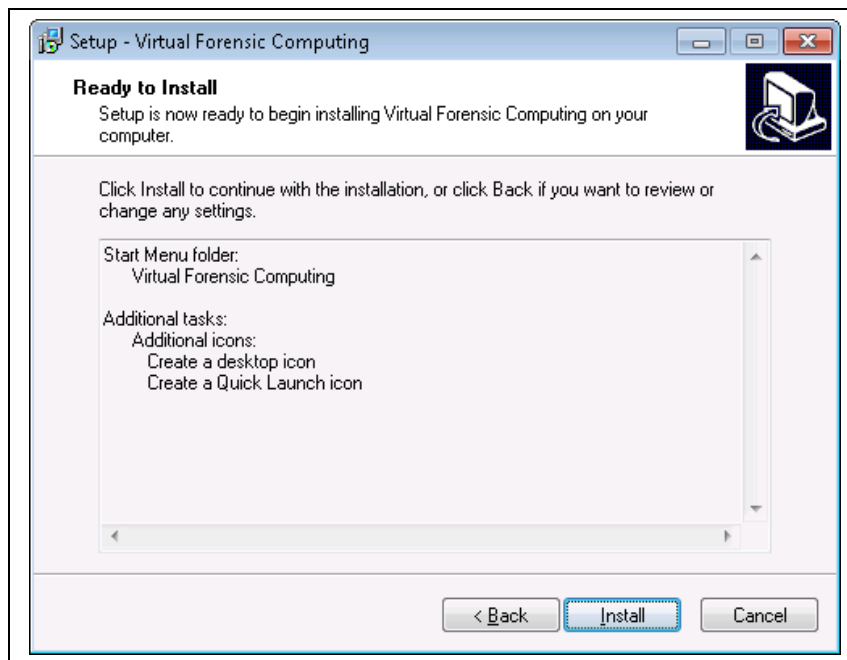
Click 'Next' and specify the location for installation or accept the default name and location. The default location will either be 'Program Files' or 'Program Files (x86)' depending on your Host OS. It is recommended that you accept the defaults.



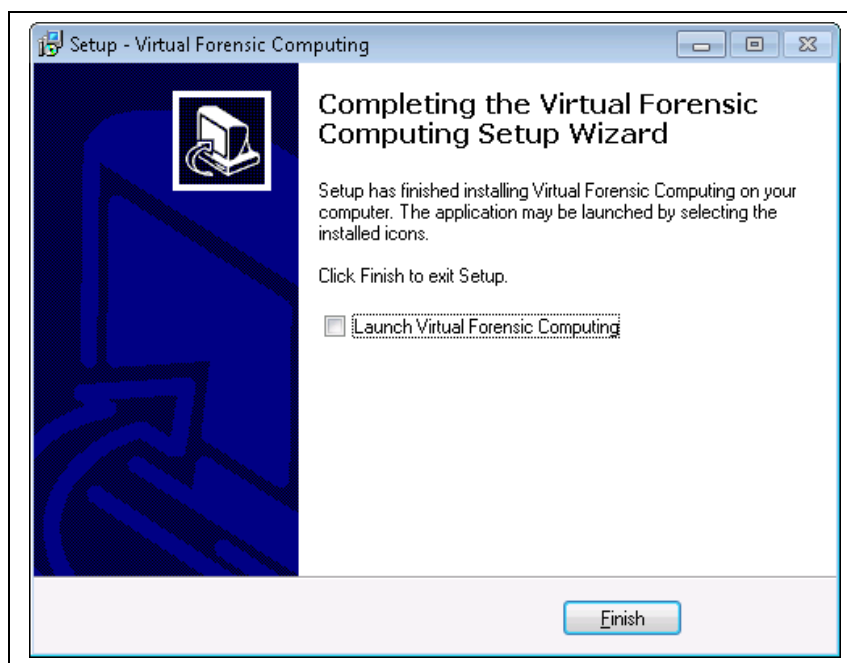
You can elect not to create a Start Menu folder if desired. Click 'Next' to proceed.



Select (or deselect) the options to create Desktop and Quick Launch icons. Click 'Next' to proceed.

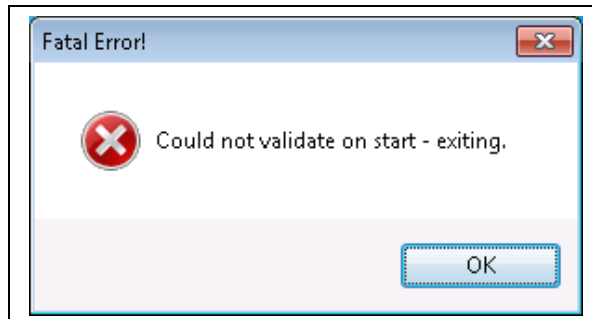


Review your installation options and click 'Install' to complete the installation of the VFC application.



De-select the option to Launch Virtual Forensic Computing and click Finish.

You will need to install both a VMware desktop product and the VMware VDDK before VFC can be utilised. If either of these applications is not present, the VFC will fail to start with the following error message.



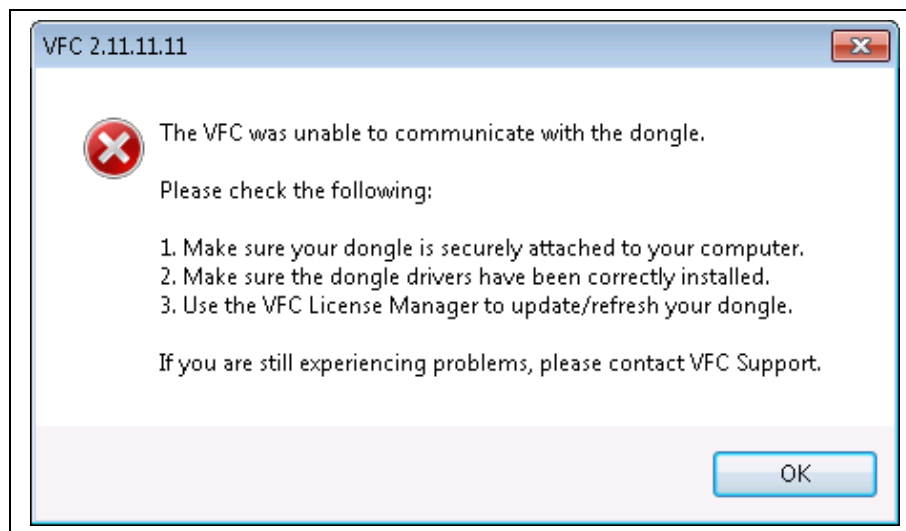
## **The VFC Dongle and Dongle Drivers**

You will need to have the VFC dongle inserted to run VFC.

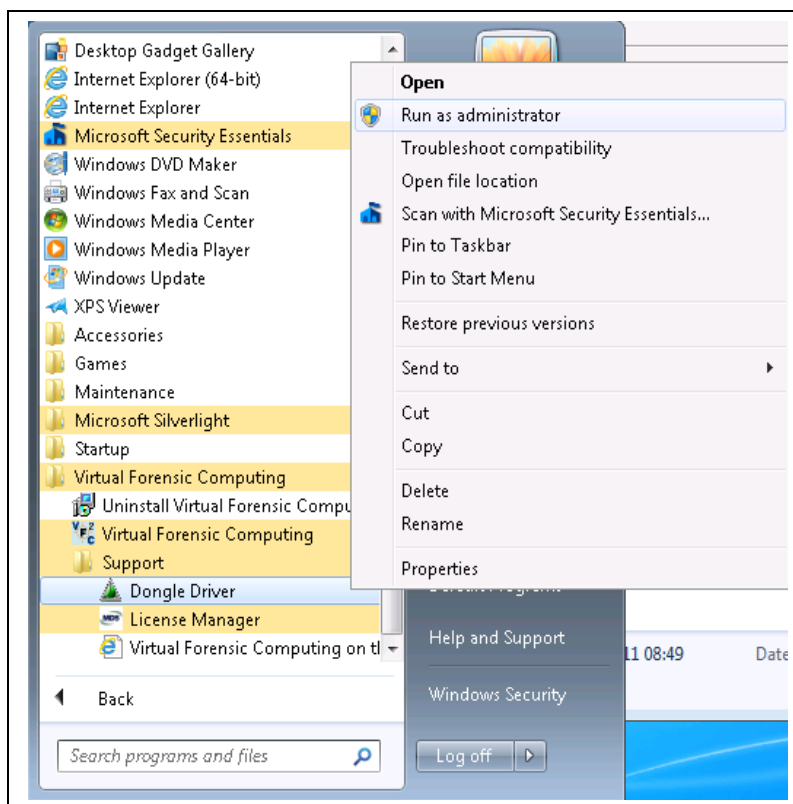
If you have a green VFC dongle, you will also need to install the required dongle drivers. If you have a white VFC dongle, this is driverless and should function without issue.

The Dongle Drivers are also required in order to use the VFC License Manager application (used to refresh the Dongle data upon renewal of a subscription).

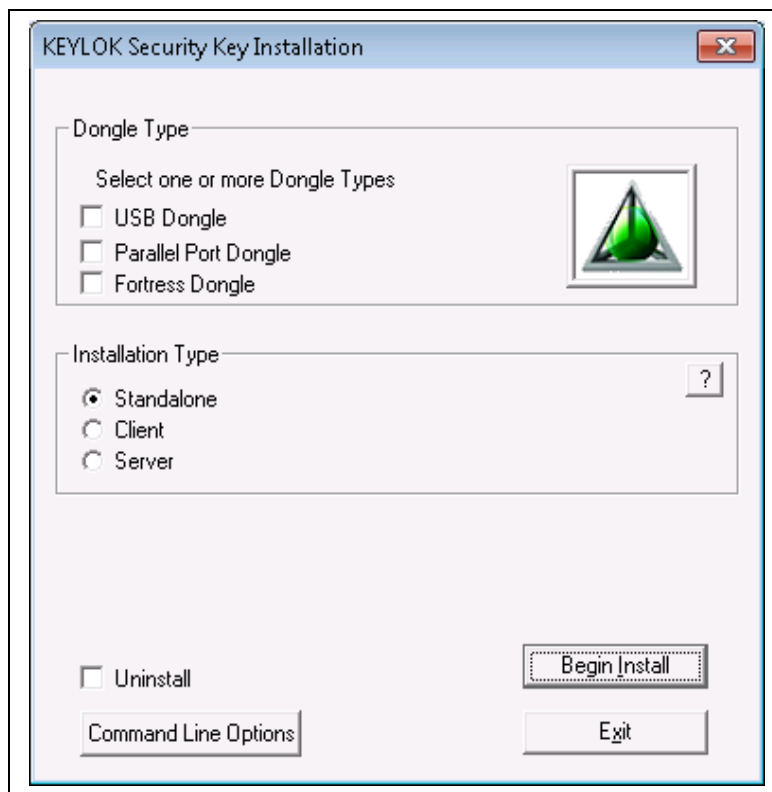
If you attempt to run VFC without a dongle, or with a green dongle and the dongle drivers have not been installed, you will see the following error message.



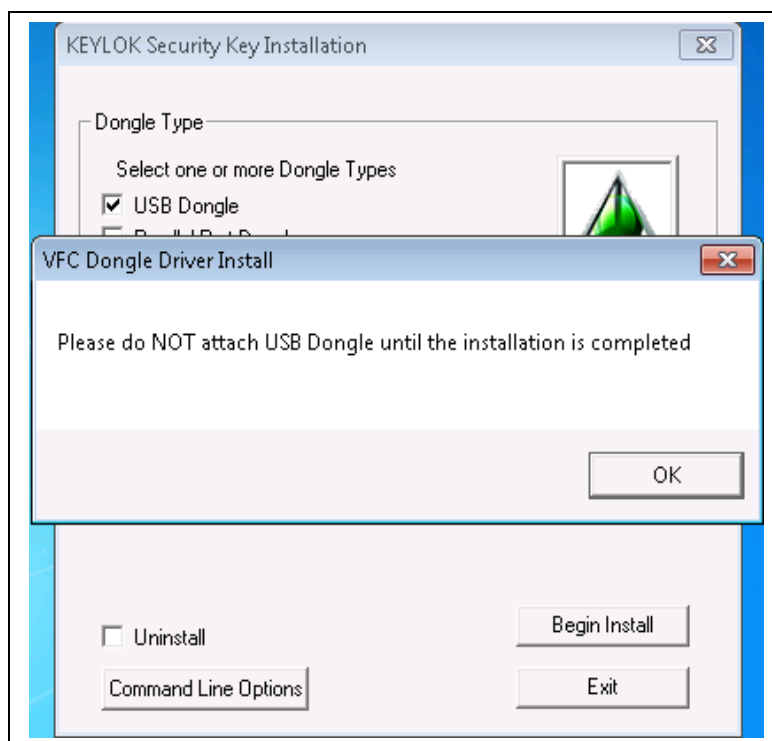
The VFC Dongle drivers can be located via the Start Menu / All Programs in the support sub-folder of Virtual Forensic Computing. **You must remove the dongle from the Host machine prior to installing the dongle drivers.**



Right click on the appropriate Start Menu shortcut and select 'Run as administrator'.

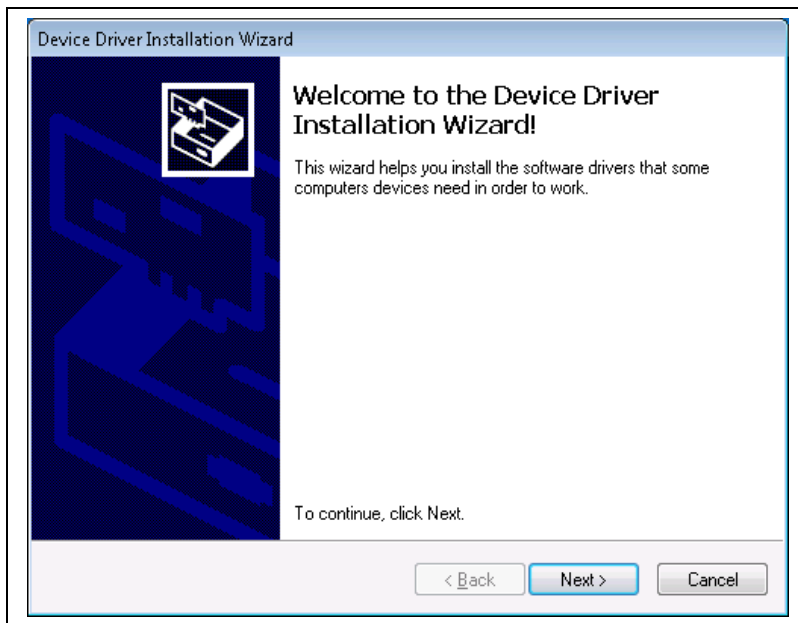


Select USB Dongle

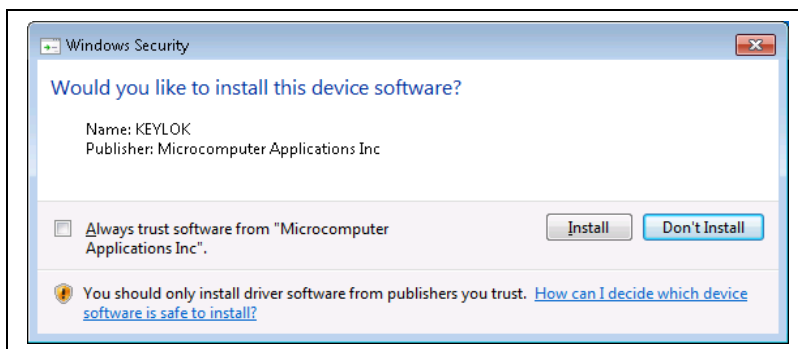


Click 'OK', then click 'Begin Install'.

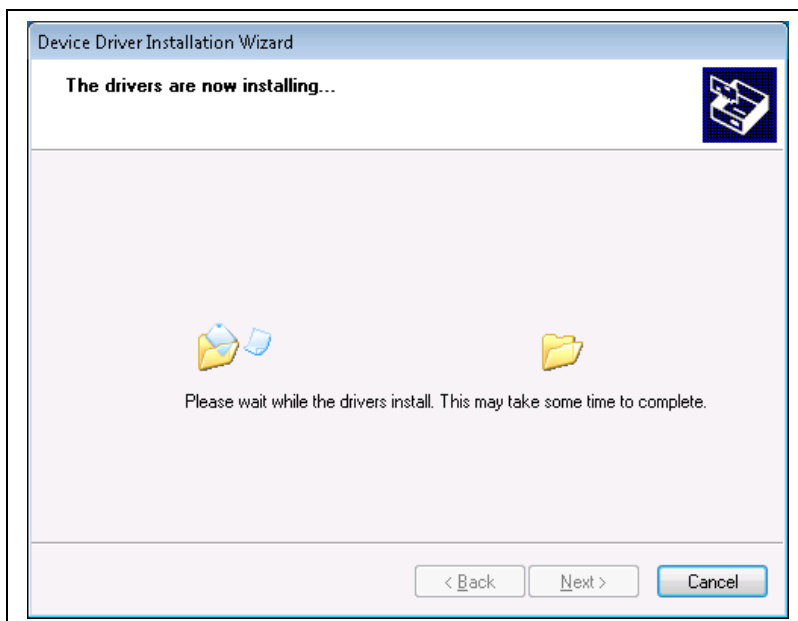


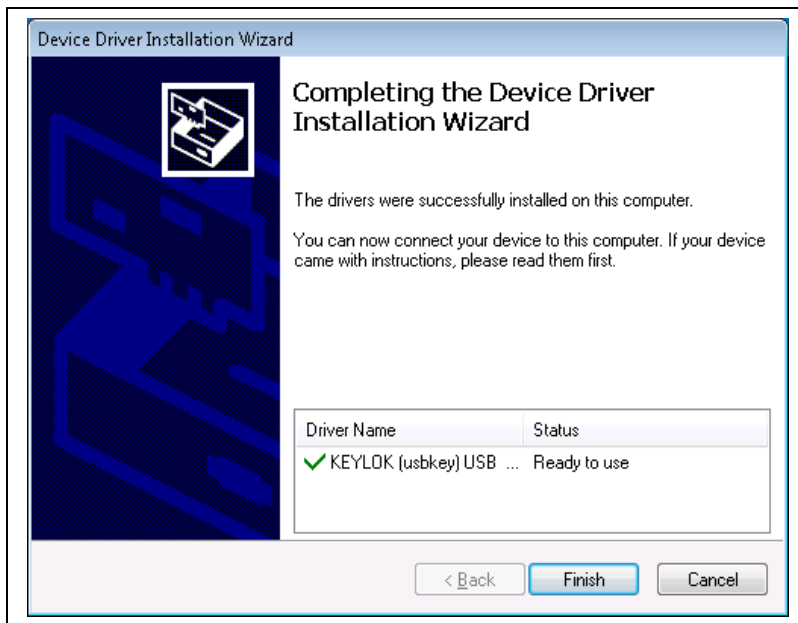


Click 'Next'

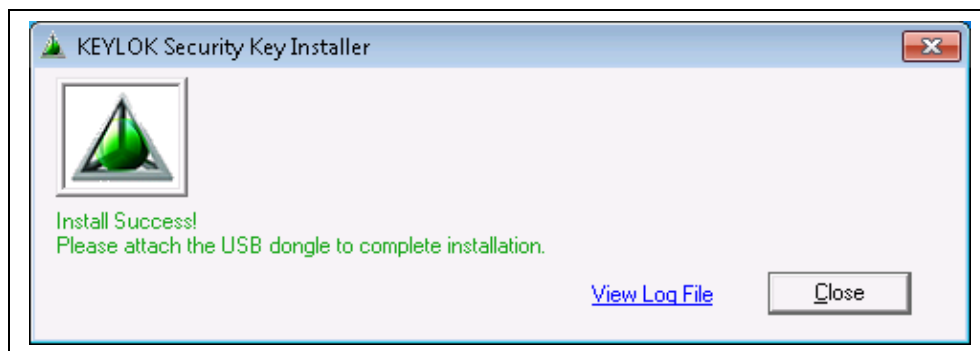


Click 'Install'





Click 'Finish'.



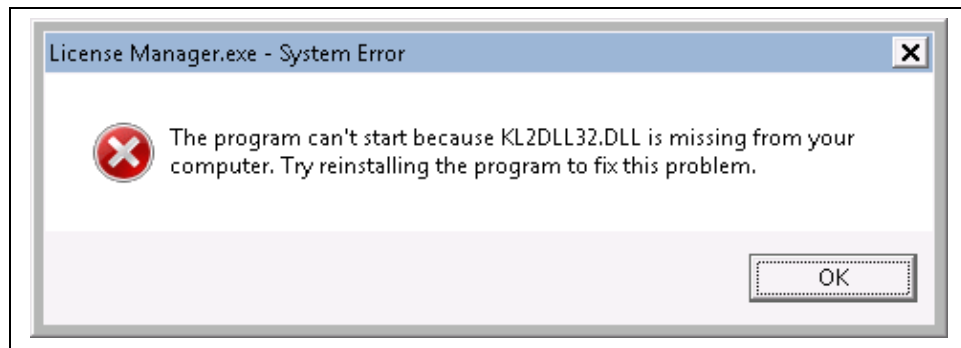
Click 'Close'.

You can now insert the VFC (green) dongle and it will be recognised, or you can run the VFC License Manager (either green or white dongle).

### **The VFC License Manager**

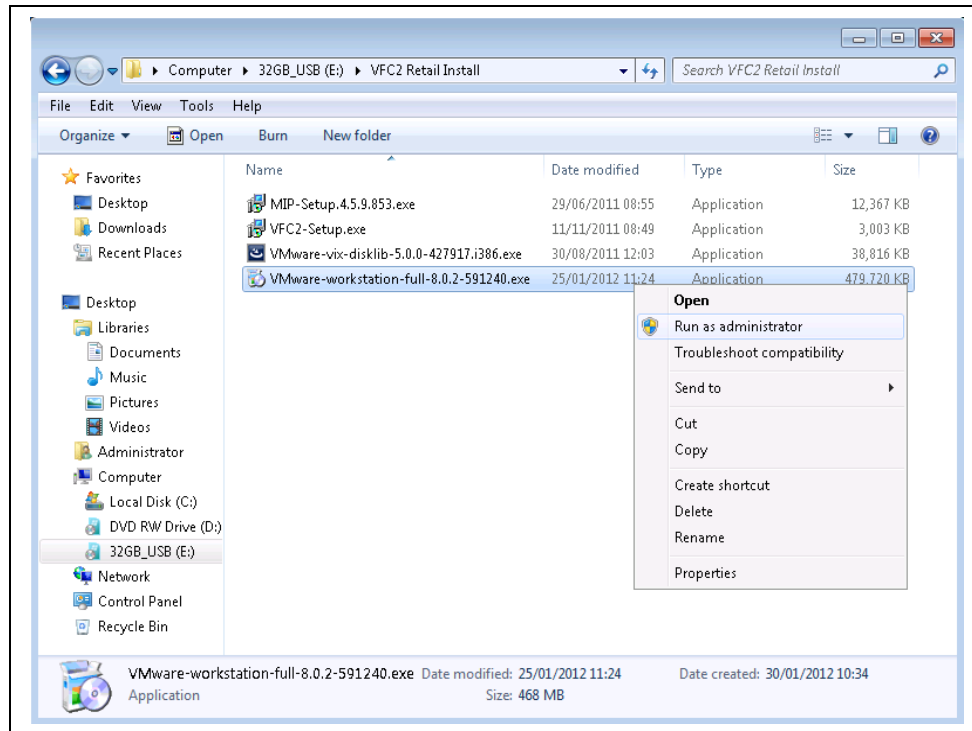
The VFC License Manager is used to refresh the dongle data when the subscription has been renewed on a registered dongle. The License Manager requires access to the Internet and utilises the settings set within Internet Explorer on your host system.

If you attempt to run the VFC License Manager without the Dongle Drivers installed, you will most likely see the following error message.

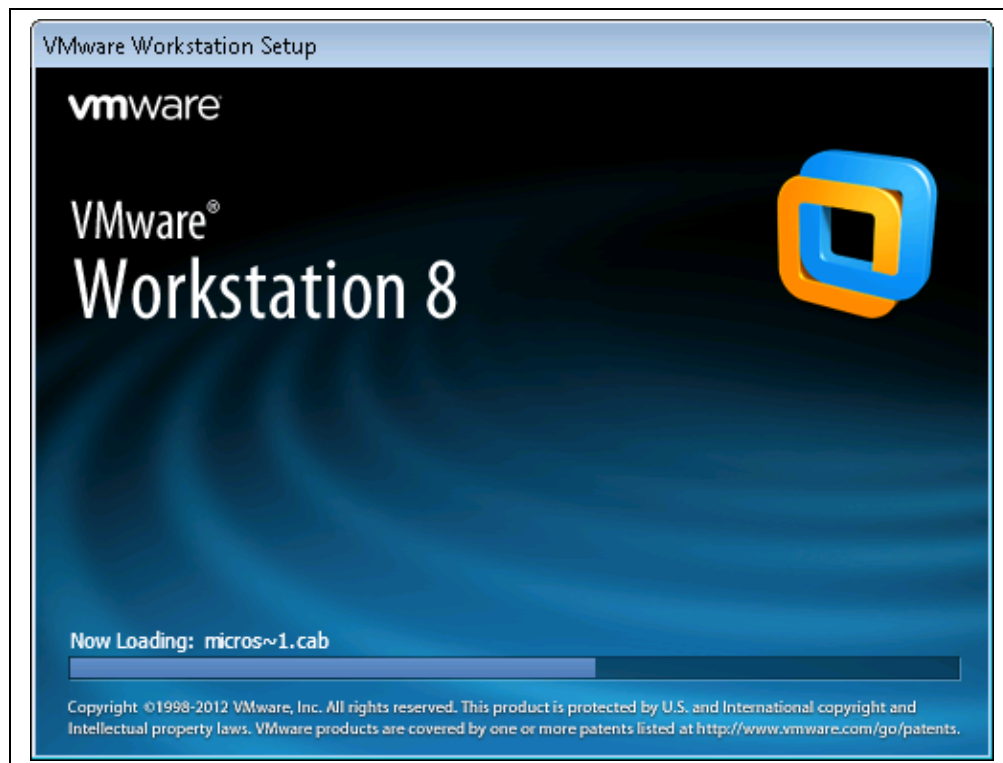


Installing the dongle drivers should resolve this issue regardless of the type of dongle you have.

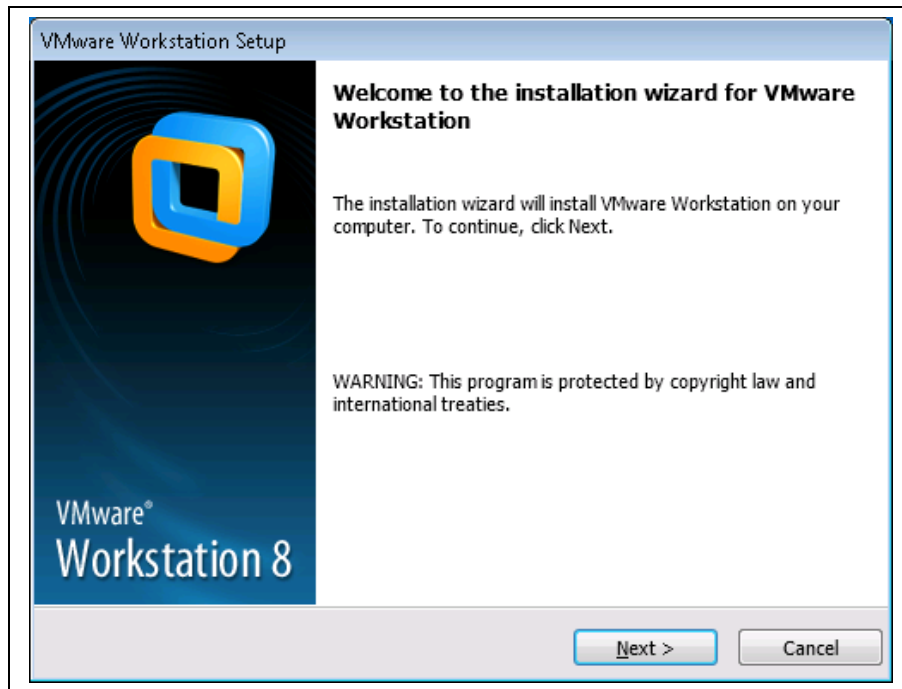
## Installation of VMware Workstation



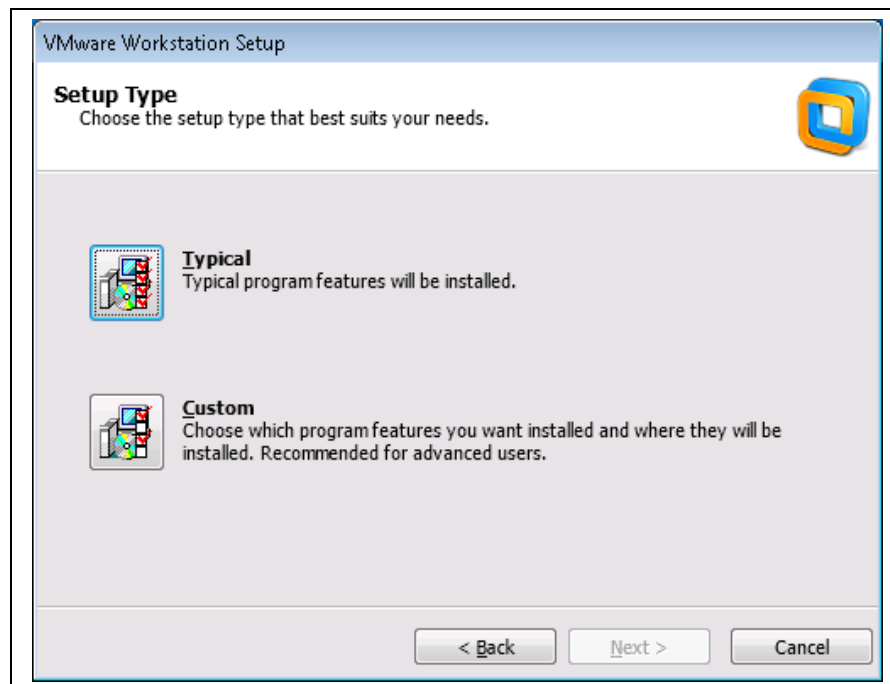
In Windows Explorer, navigate to the location where you have saved the installation files, right-click on the VMware-workstation-full-8.0.2-591240.exe file (or whichever version you have access to) and select 'Run as administrator'.



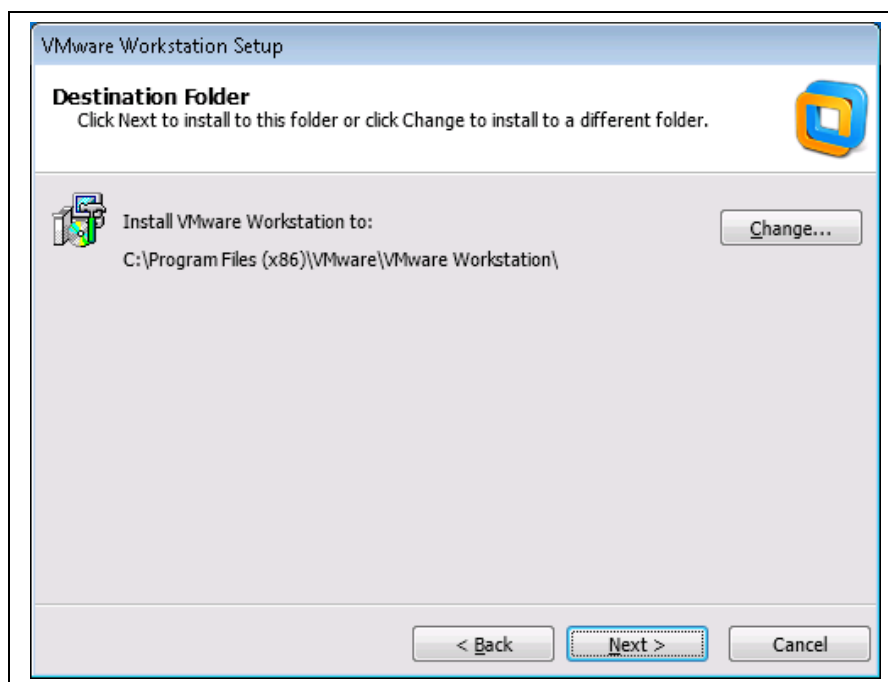
There should be little need to answer any of the installation prompts with other than 'Next'.



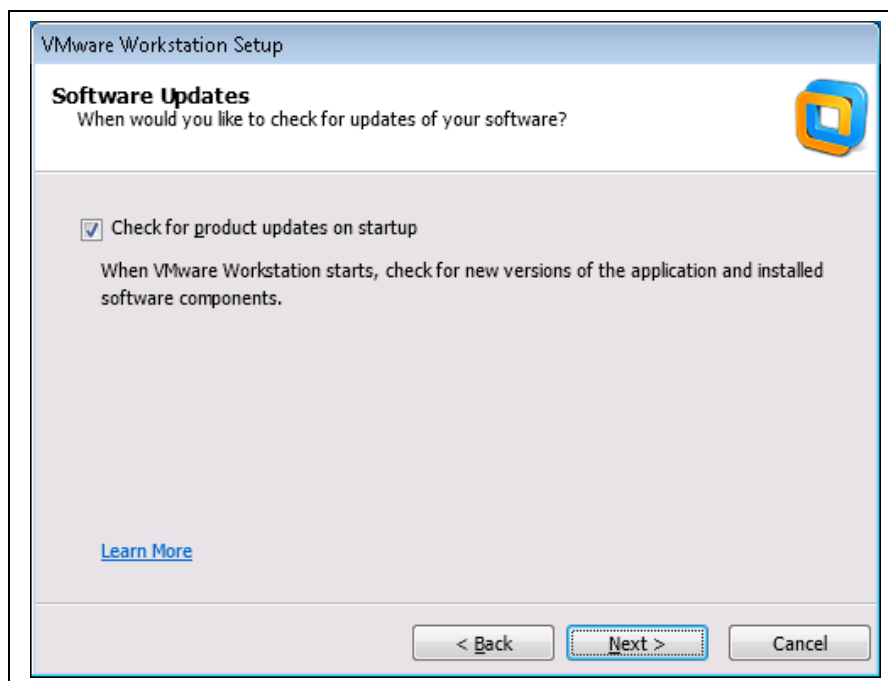
A typical installation of workstation should suffice. Click 'Next' to proceed.



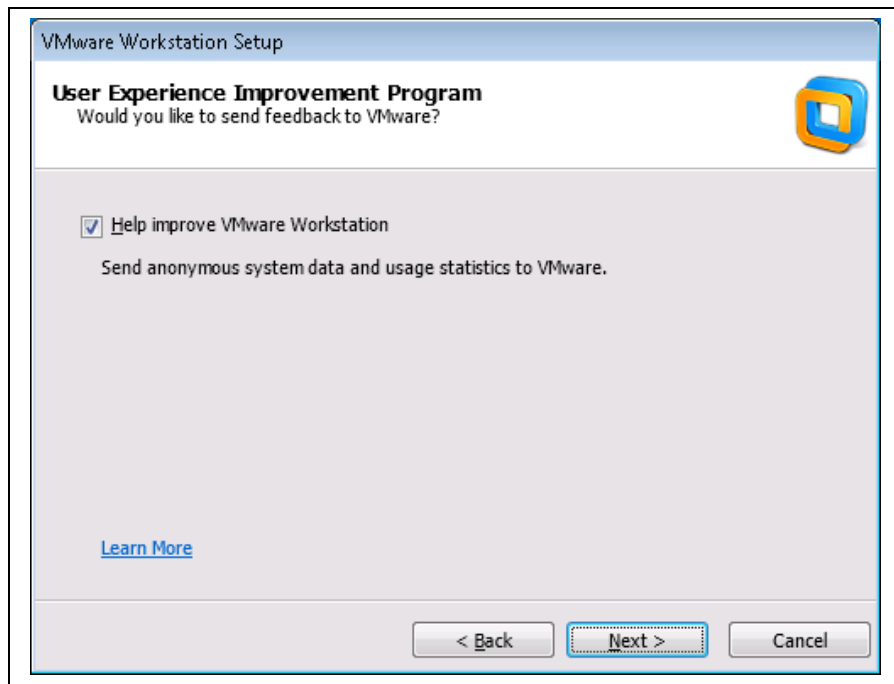
Either accept the default installation folder (recommended) or change the installation location and click 'Next'.



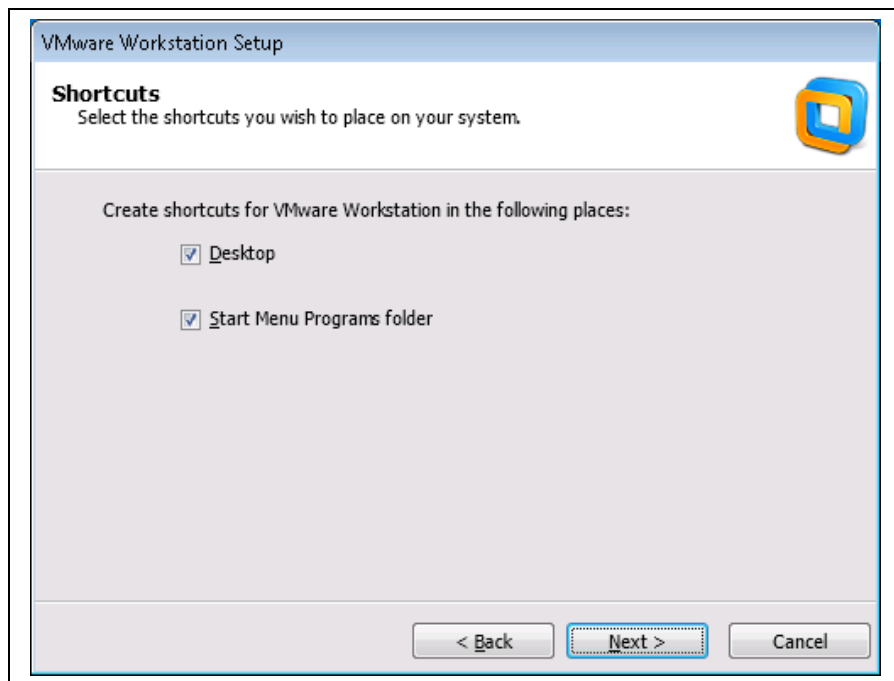
Check for product updates can be disabled if using a non-Internet connected Host System.



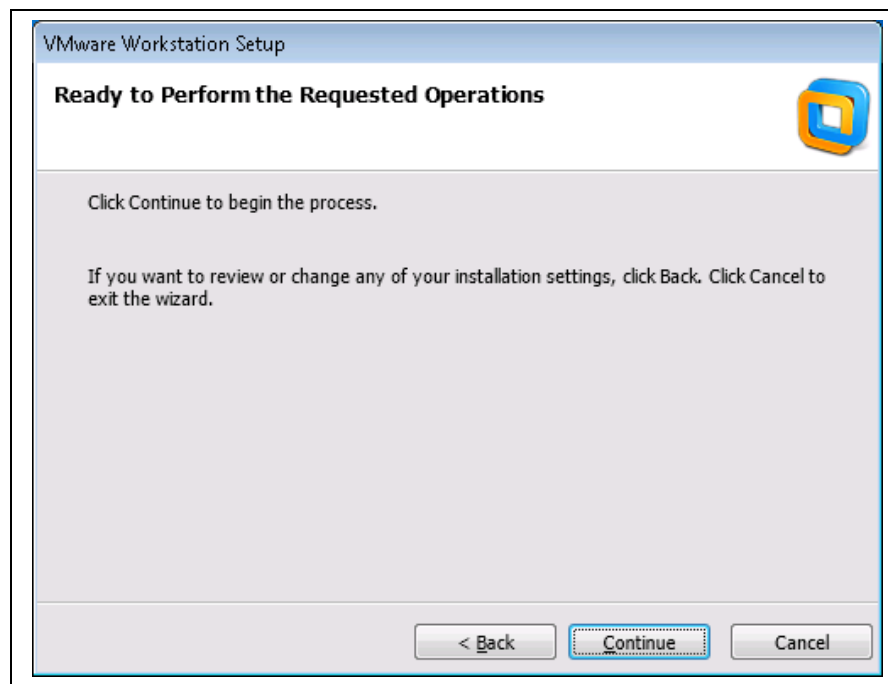
Click 'Next' to continue.



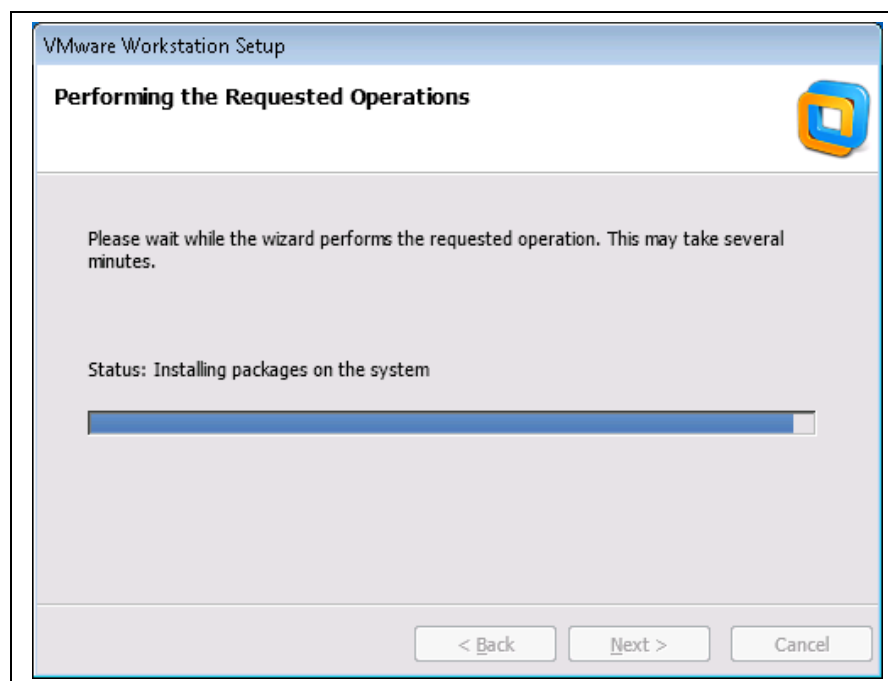
Sending system and usage data can be disabled if required. Click 'Next' to continue.



Default options for creating shortcuts on desktop and Start menu are enabled but can be disabled if required. Click 'Next' to continue.

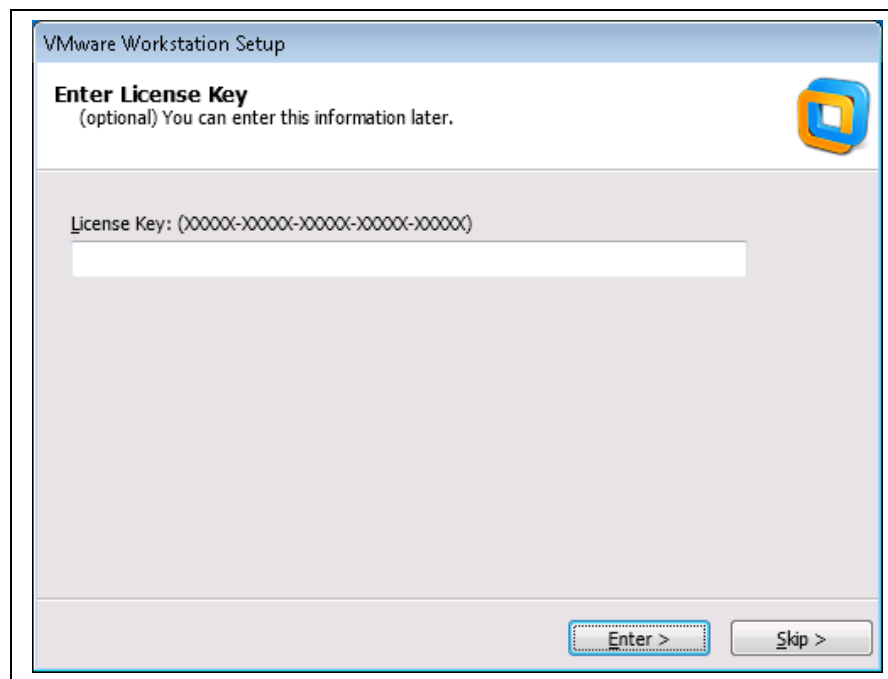


Clicking 'Continue' will start the installation process.

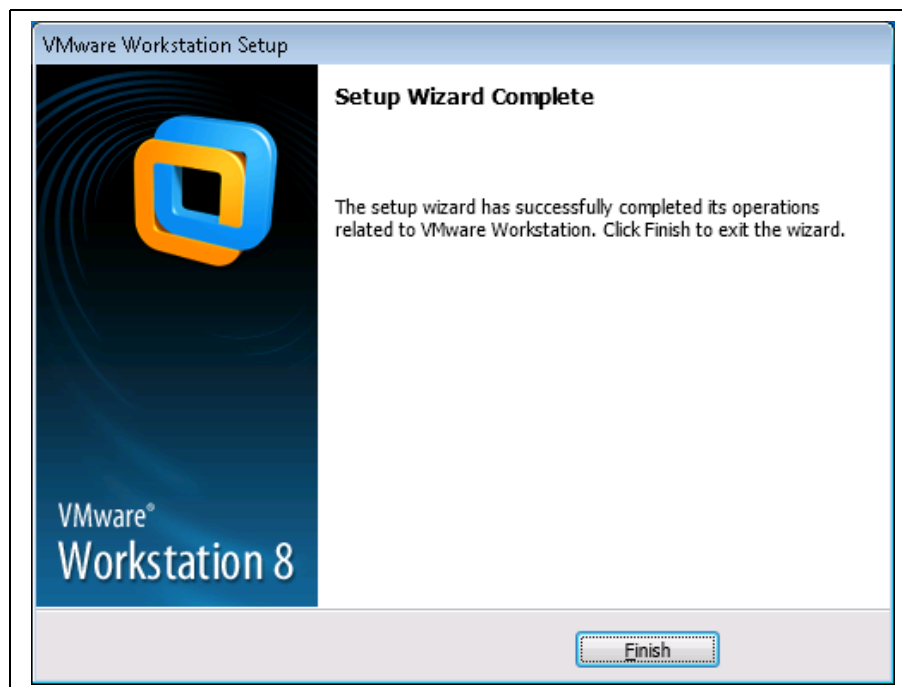


The installation can take several minutes.





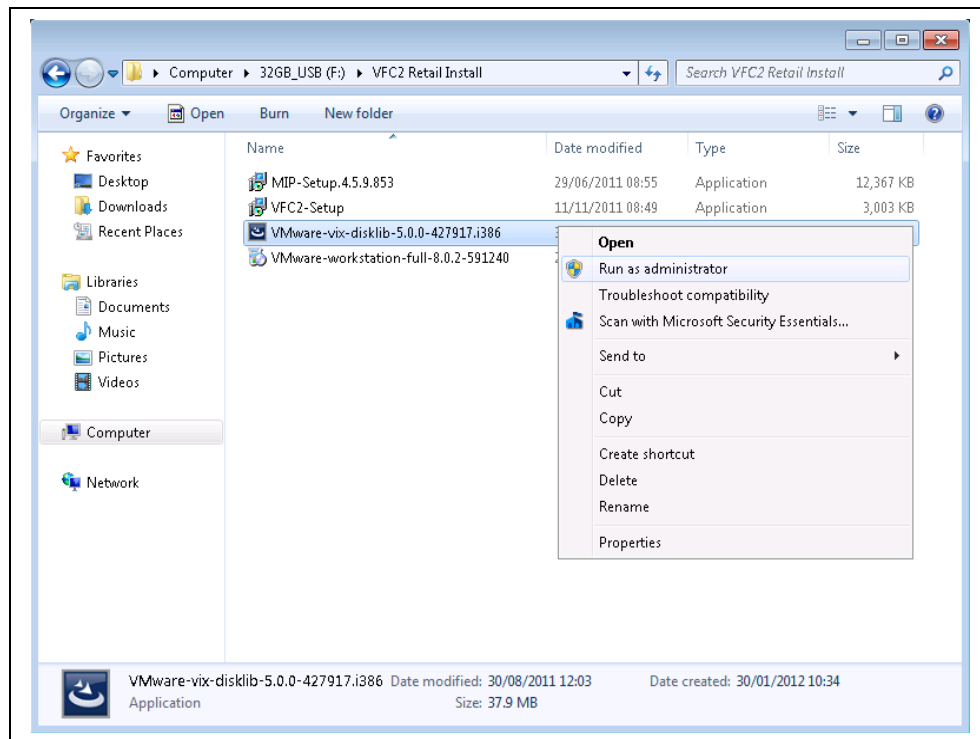
VMware Workstation requires a license registration key but can work in trial mode for up to 30 days.



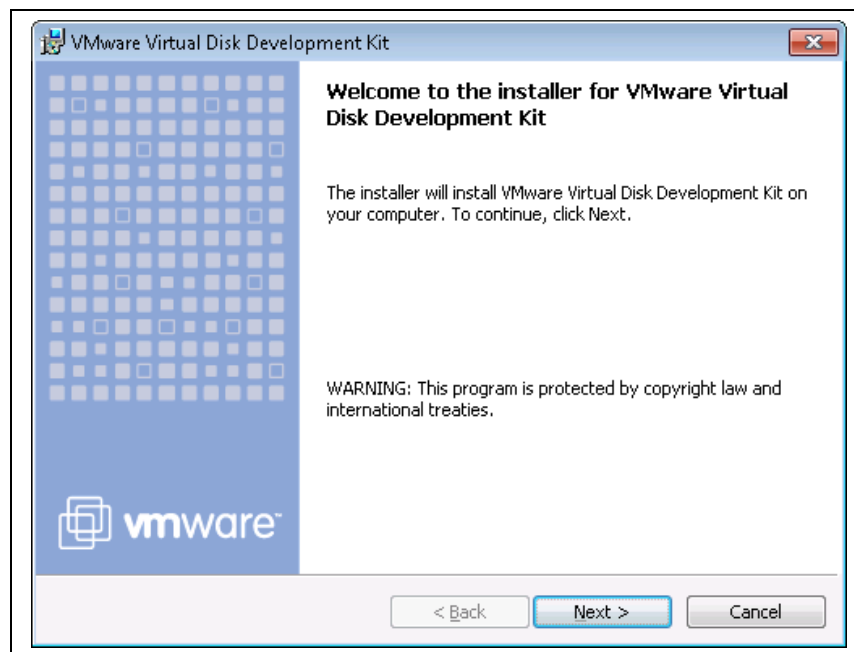
Click 'Finish' to exit the installation wizard.

## Installation of VMware VDDK

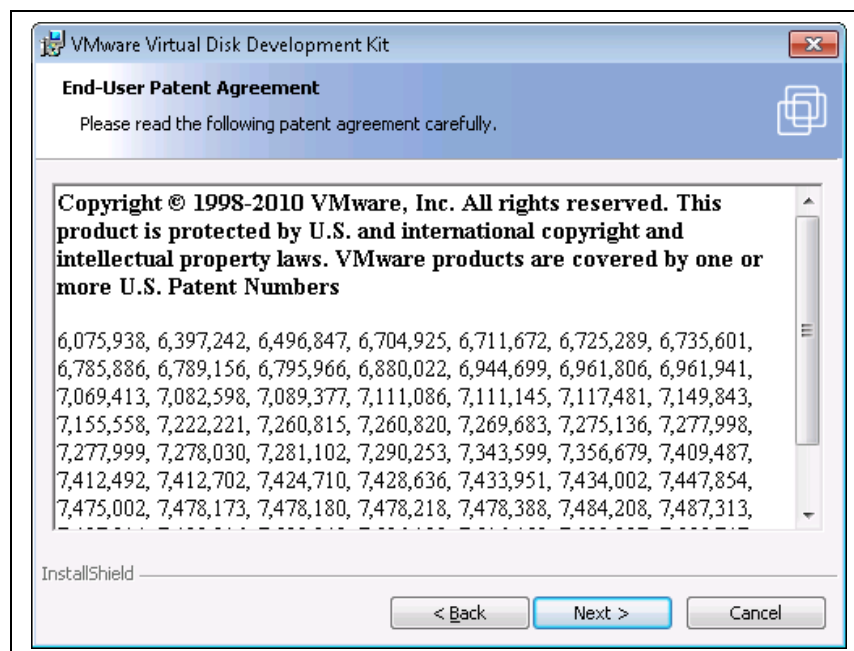
It is highly recommended that the latest version of the VMware VDDK is used.



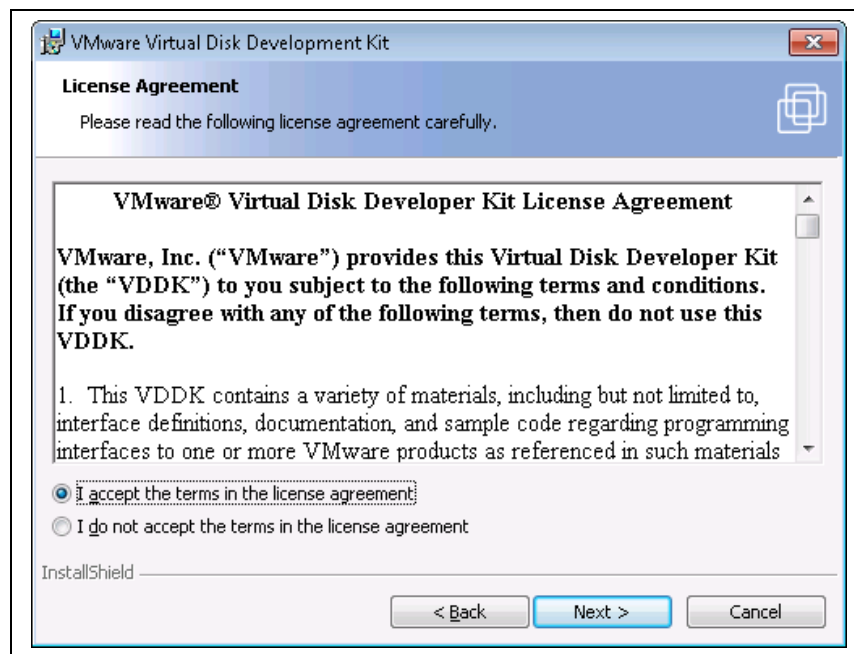
In Windows Explorer, navigate to the location where you have saved the installation files, right-click on the VMware-vix-disklib-5.0.0-427917.i386.exe file (or whichever version you have access to) and select 'Run as administrator'. Please note that earlier versions of this application are not guaranteed to work with VFC as expected and as such are unsupported.



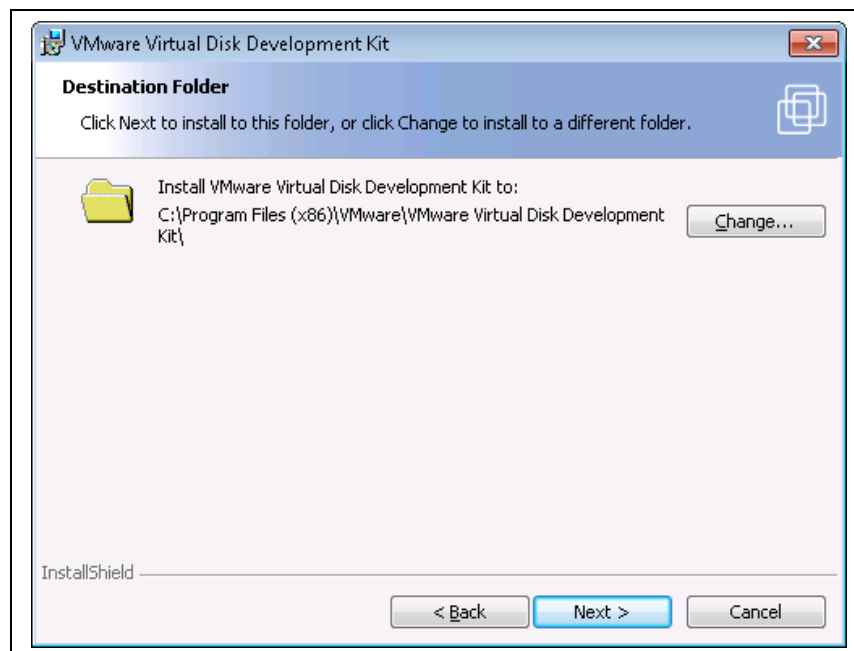
Click 'Next' to continue.



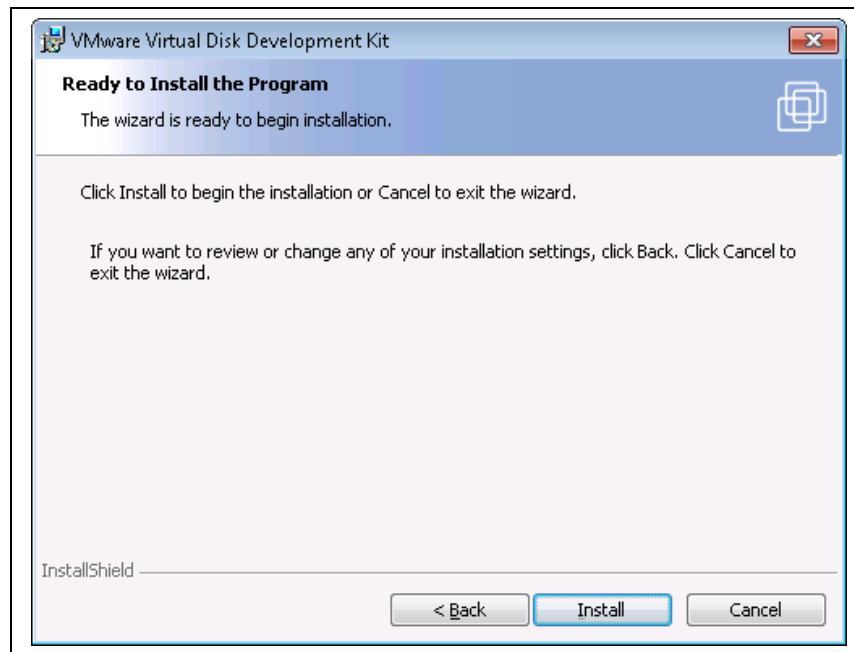
The End User Patent Agreement will be displayed. Click 'Next' to continue.



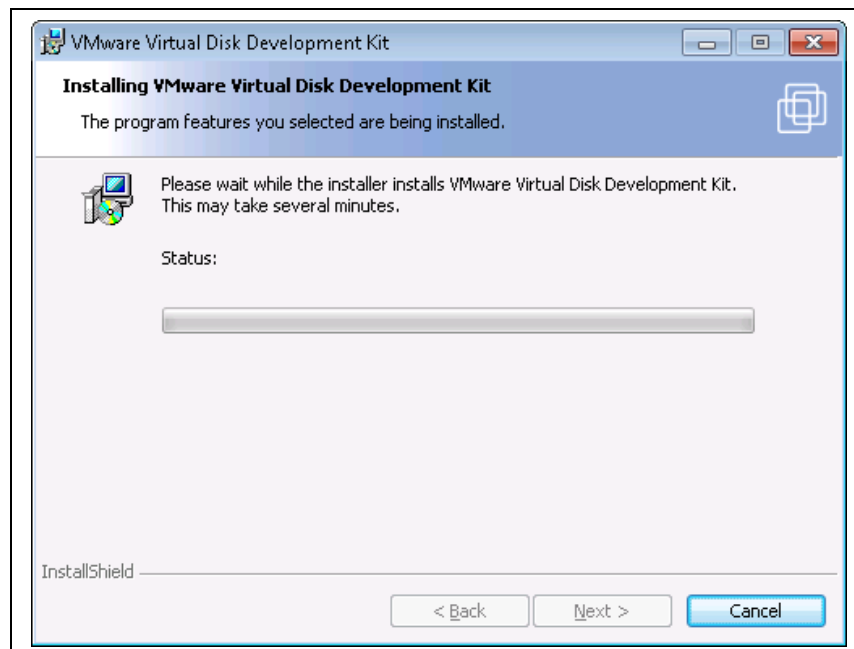
The End User License Agreement will be displayed. Accept the terms and Click 'Next' to continue.



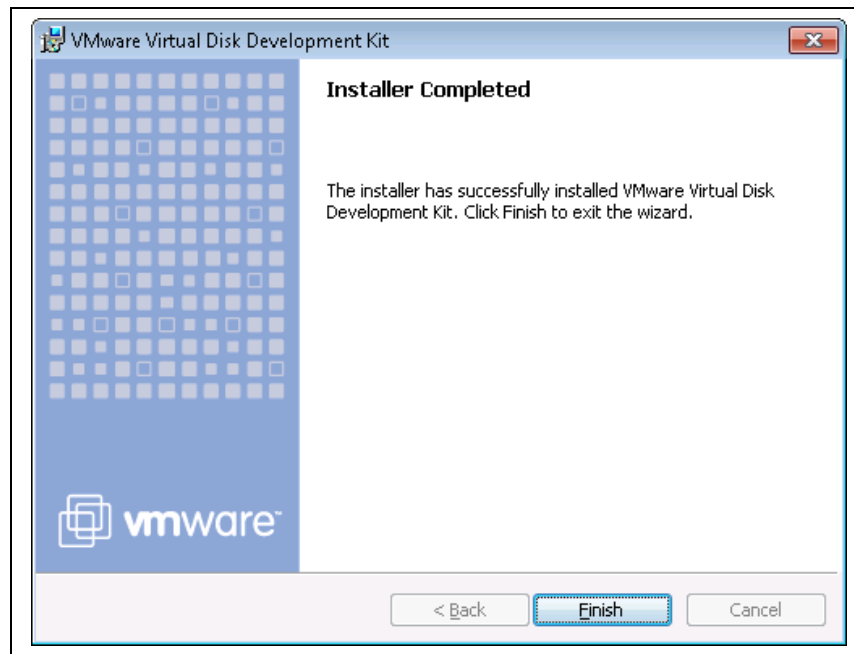
You can either accept the default installation folder (recommended) or change the installation location and click 'Next'.



Click 'Install' to begin the installation process.

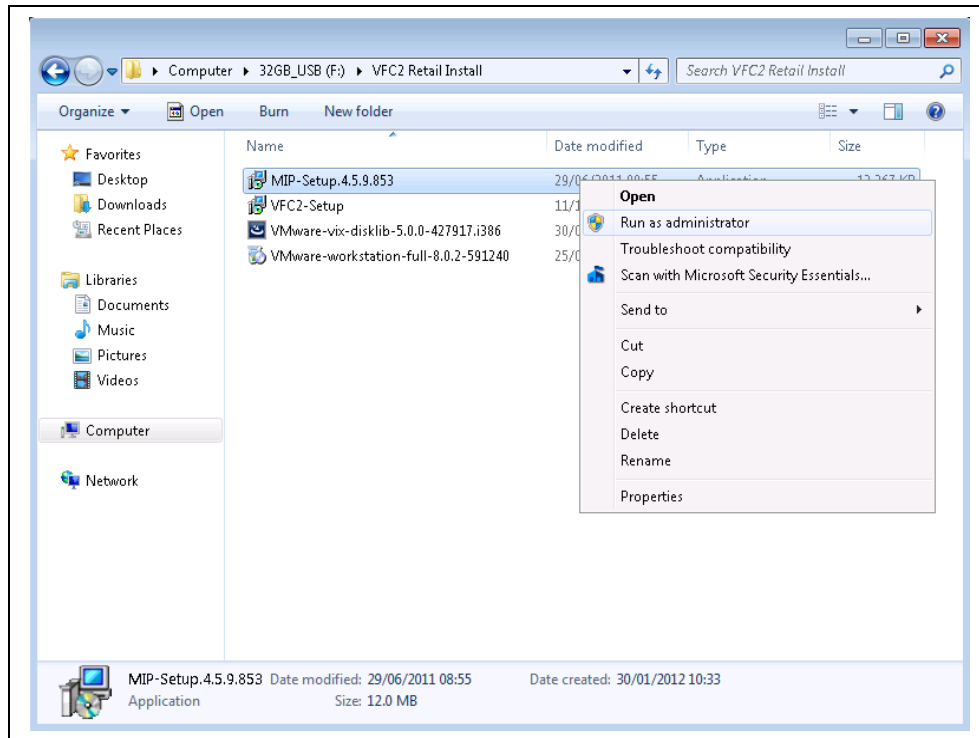


The installation may take several minutes.



Click 'Finish' to exit the installation wizard.

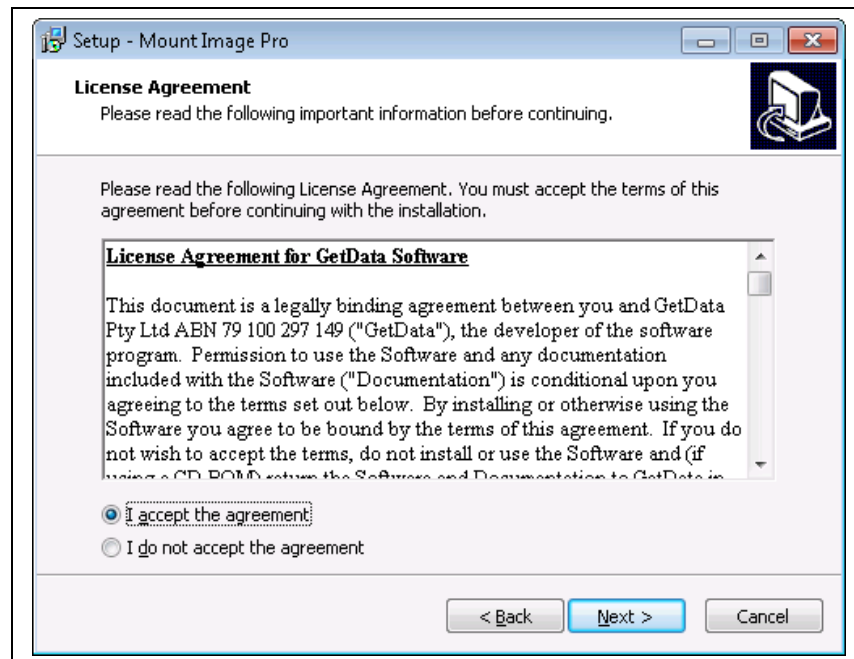
## Installation of Mount Image Pro



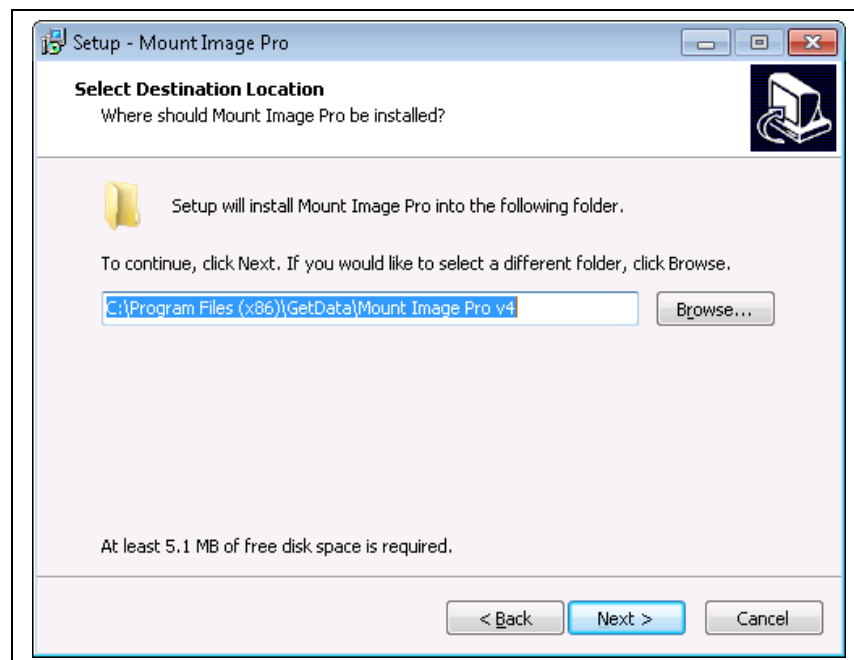
In Windows Explorer, navigate to the location where you have saved the installation files, right-click on the MIP-Setup.4.5.9.853.exe file (or whichever version you have access to) and select 'Run as administrator'. Please note that earlier versions of this application are not guaranteed to work with VFC and as such are unsupported.



Click 'Next' to continue.

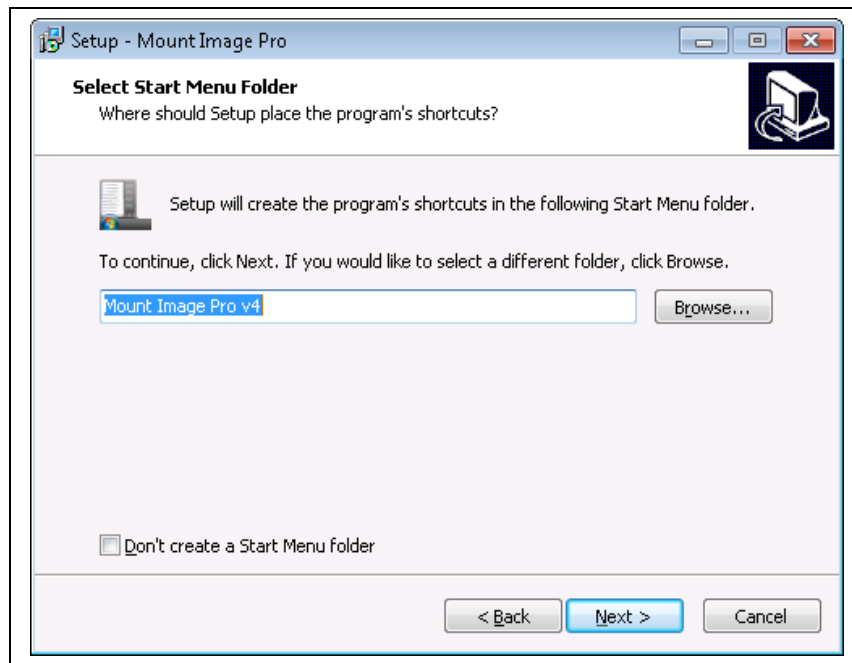


The License Agreement will be displayed. Accept the terms and Click 'Next' to continue.

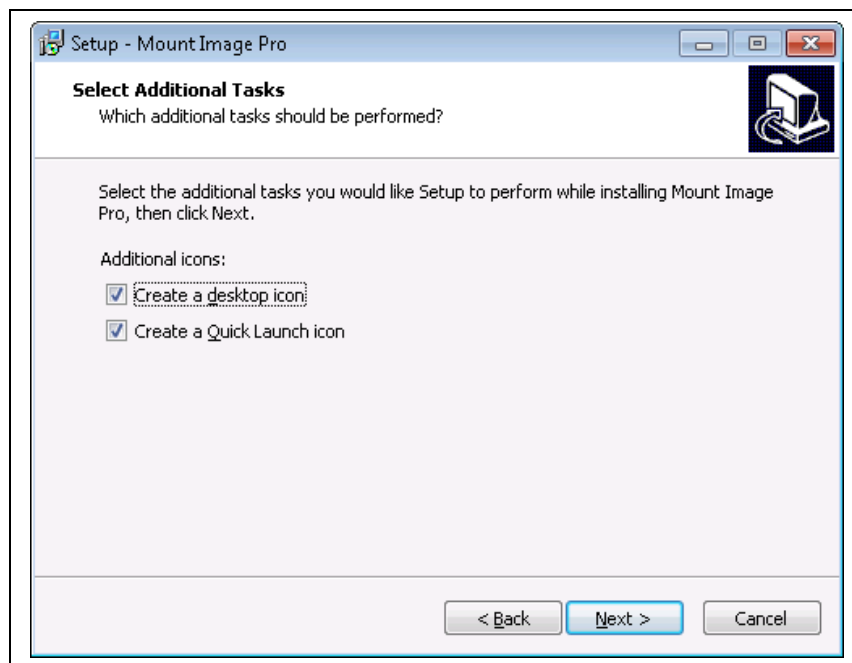


You can either accept the default installation folder (recommended) or change the installation location and click 'Next'.

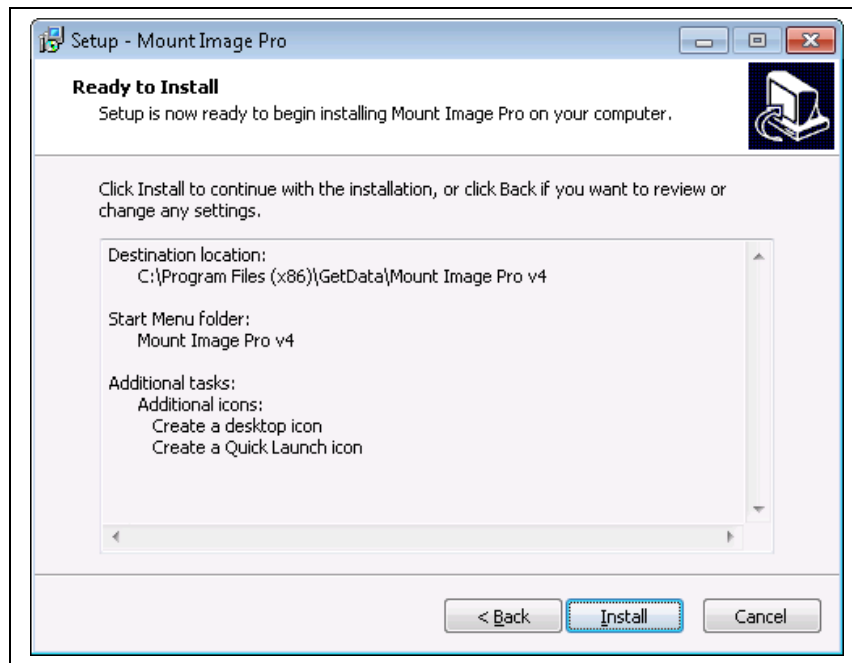




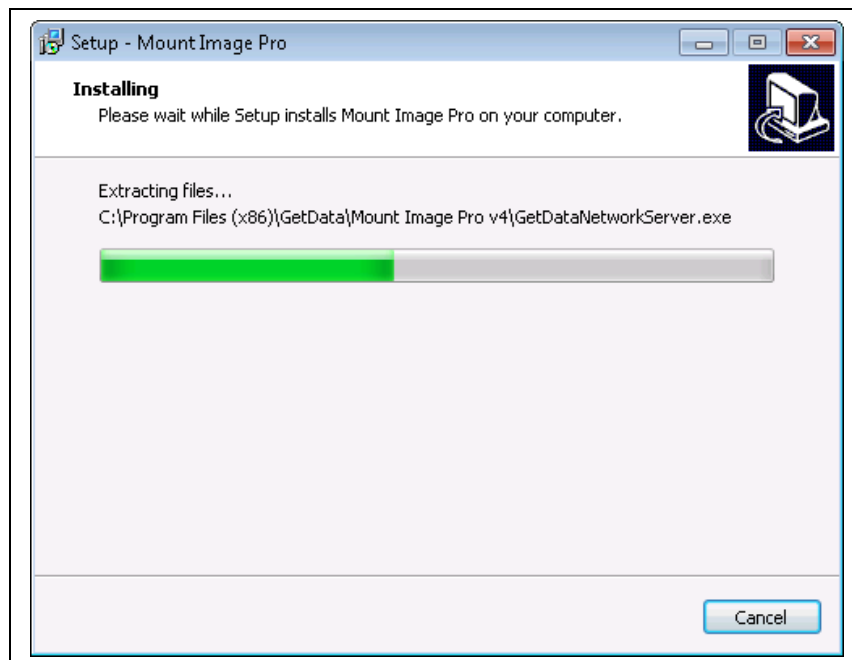
You can either accept the default Start Menu folder (recommended) or change the name of this folder and click 'Next'.



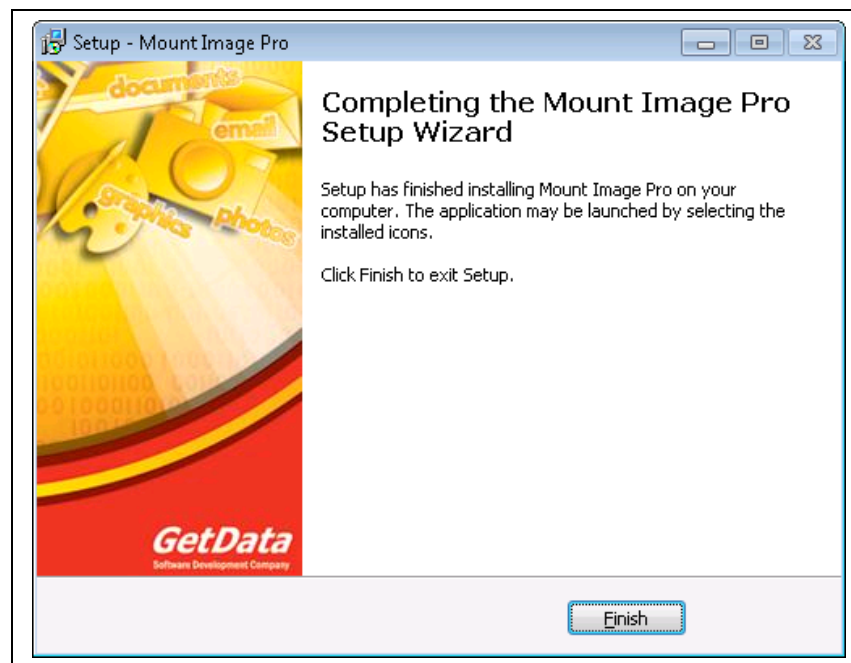
Select (or deselect) the options to create Desktop and Quick Launch icons. Click 'Next' to proceed.



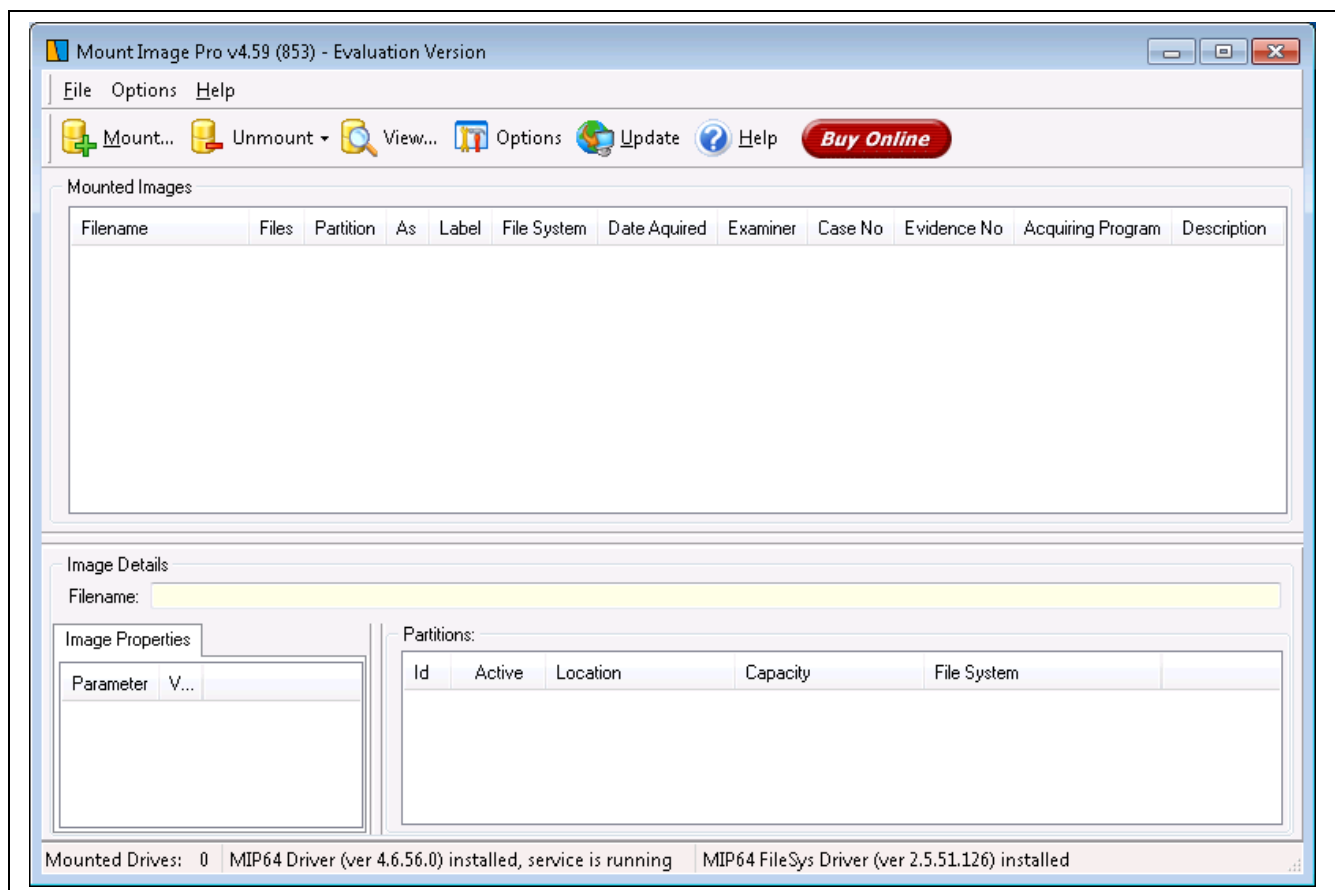
Click 'Install' to begin the installation process.



The installation may take several minutes.



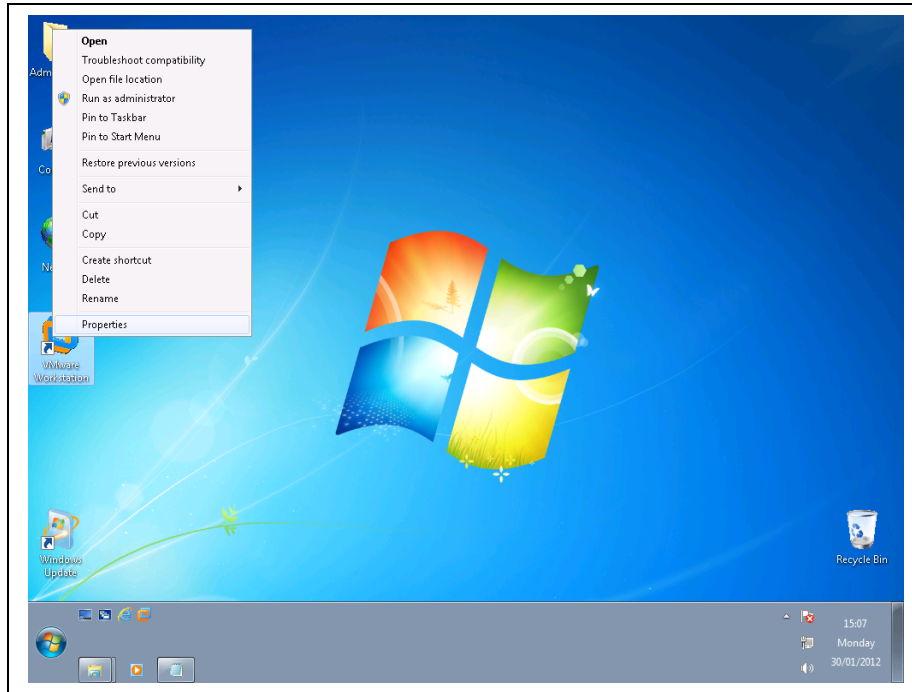
Click 'Finish' to exit the installation wizard.



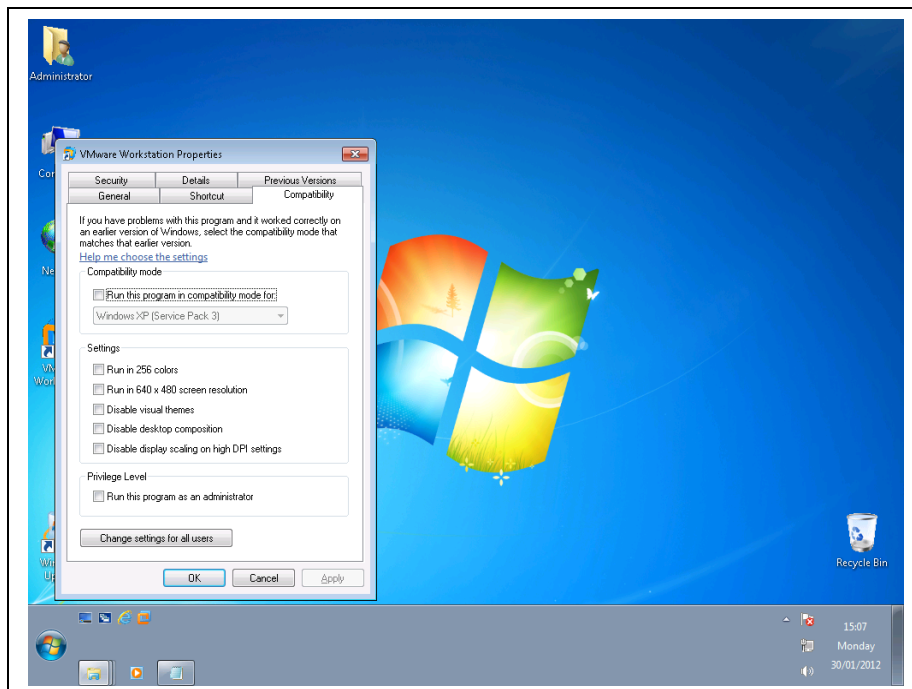
Mount Image Pro requires a license registration key or a license dongle (separate from the VFC dongle) but it can work in Evaluation Mode for up to 15 days.

## *Change Application Shortcuts to 'Always run as administrator'.*

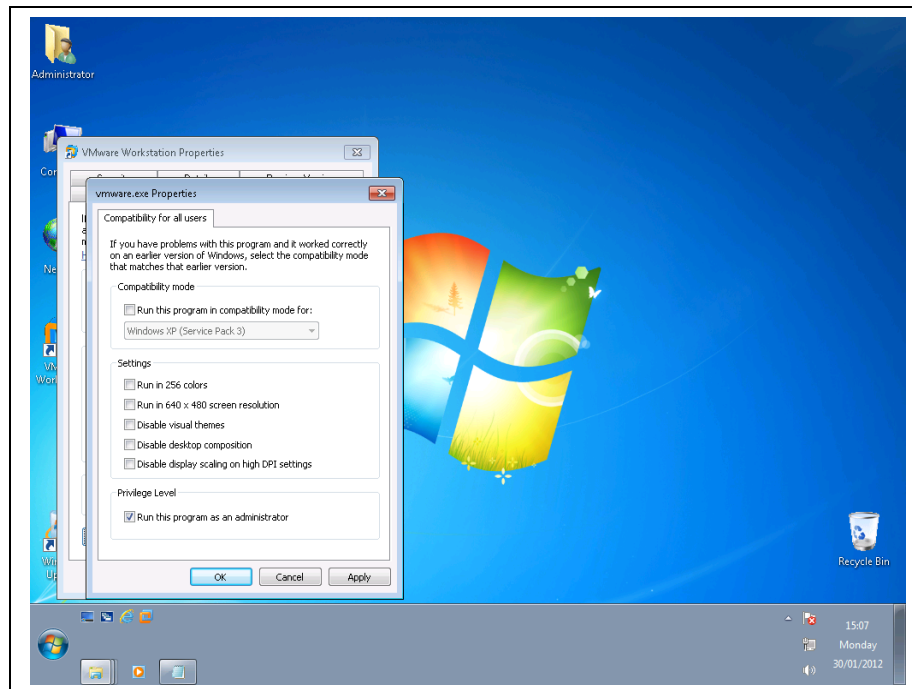
When all relevant applications have been installed, it is useful to change the properties of any desktop icons that are used to subsequently launch the programs such that they, too, are set to 'Always Run as Administrator'.



Right-click on the relevant desktop icon and select properties.



Either check the 'Run this program as an administrator' or, if using a workstation which multiple users may have access to, select 'Change settings for all users'.



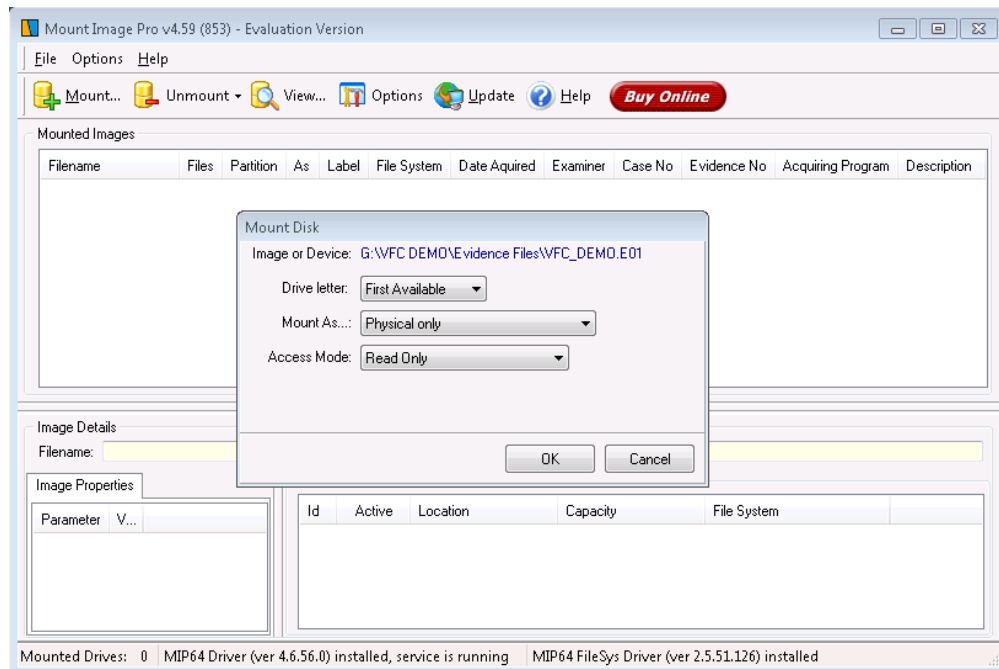
Check the 'Run this program as an administrator' option and click 'OK'.

Repeat these steps for the desktop icons (and Quick Launch icons if applicable) for the VFC and MIP applications.

## VFC: Step-by-Step

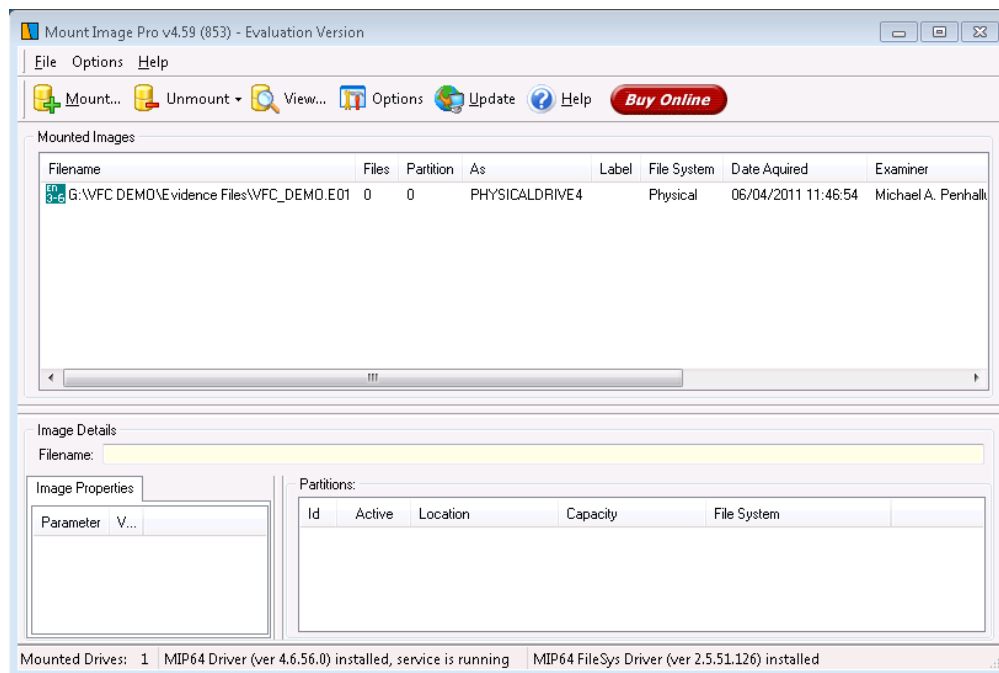
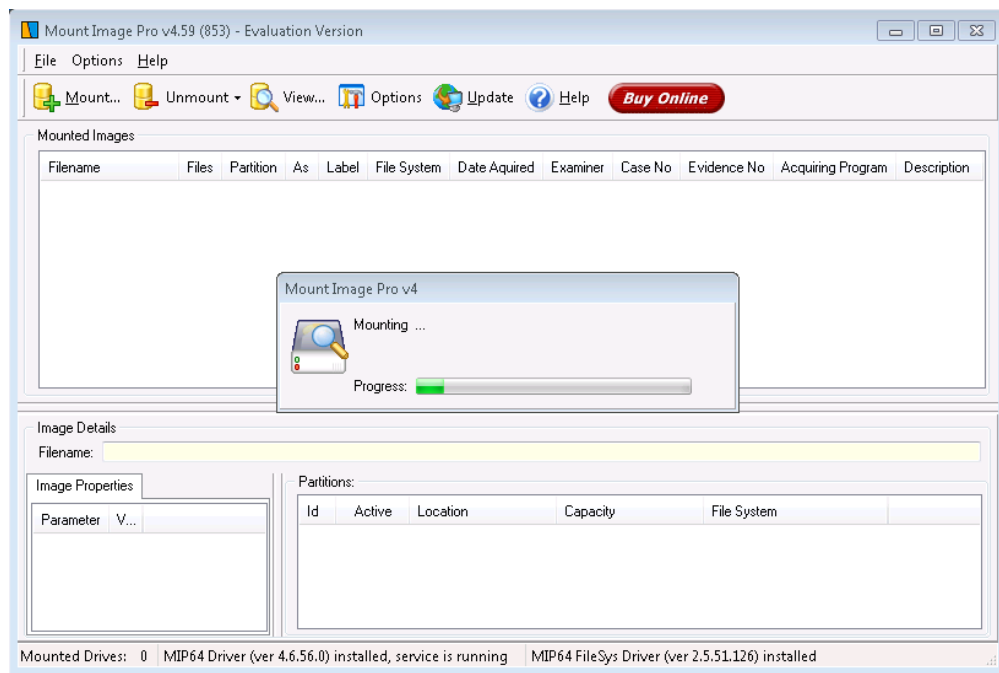
### *Mount a forensic whole disk image*

There are several methods by which a forensic whole disk image can be mounted; the author's preferred mounting tool is Mount Image Pro and the drag-and-drop mode whereby the first image file (\*.E01) is dragged into an open MIP session and mounted as a physical disk (no associated drive letter).



Once the image has been successfully mounted, the mounting application can be minimised as no further direct interaction is required.

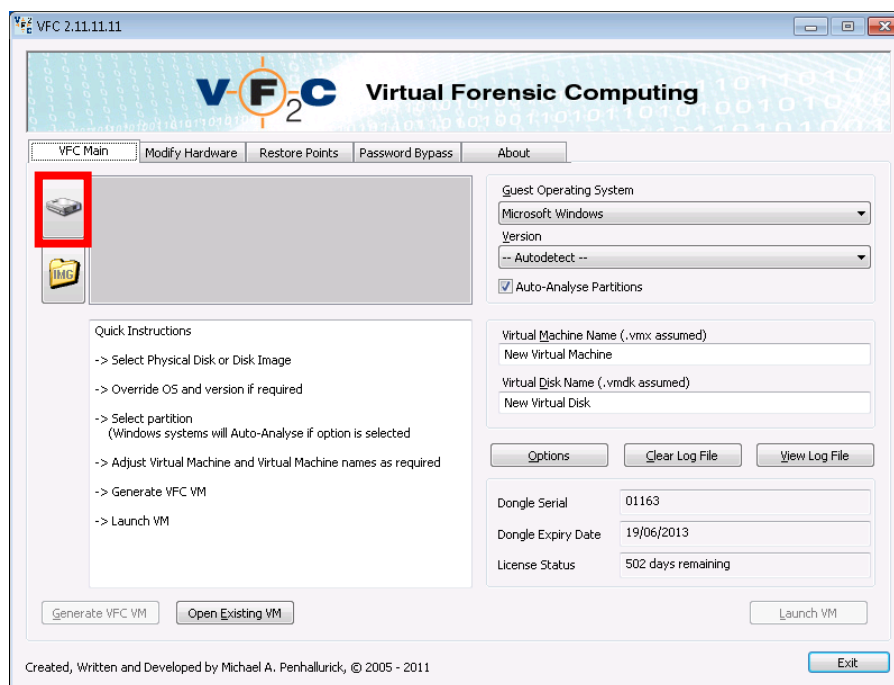
**NB** *If using either Encase PDE or the FTK Imager mount function, closing either of these applications will cause the image to dismount. The MIP GUI can be closed but will minimise the application to the system tray whilst maintaining the mounted status of the image.*



As can be seen from the above, the VFC\_DEMO.E01 image has been mounted as PHYSICALDRIVE4 and is now available to the system.

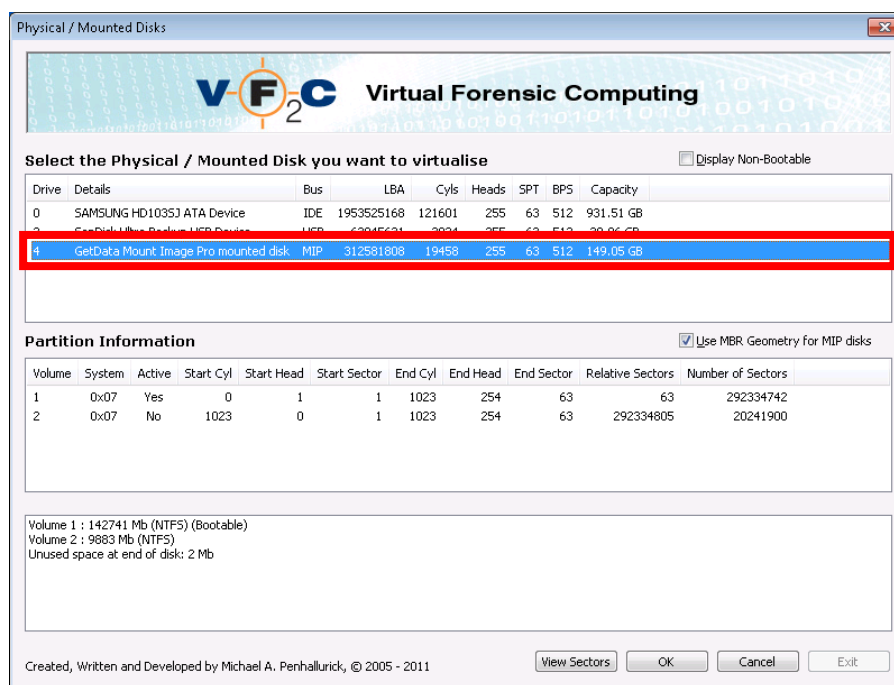
From this point, the MIP GUI is no longer directly required by VFC and can be minimised.

## Select Source Device – Mounted Hard Disk



Start VFC and use the hard disk icon located at the upper left of the screen to launch the drive selection dialog.

This process will enumerate all physical storage devices attached to the system and may take several moments.





Once enumeration is complete, the mounted drive will be displayed in the drive selection dialog.

If the mounted drive is not displayed, then VFC has been unable to ascertain that there is an active (bootable) partition present on the disk. This is most common with disks that have been used for data storage only, such as external hard disks or secondary storage devices, or with disks that do not have a standard MBR (such as Mac OS X GUID Partition systems).

*Rarely, you may need to reboot the host machine and remount the drive before it is correctly detected by VFC. This may happen when a large number of disk images have been mounted / dismantled and multiple machines have been generated.*

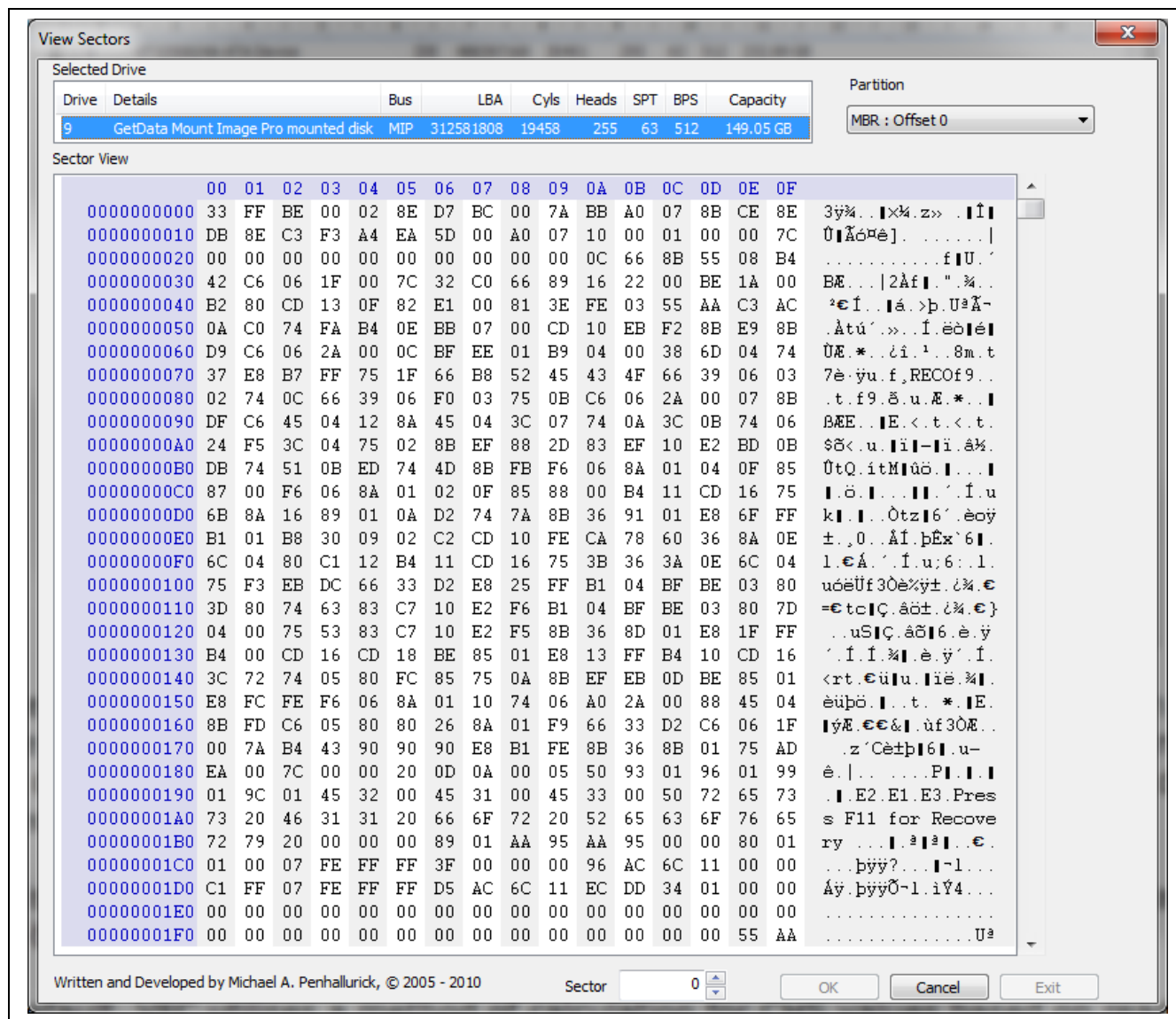
To display non-bootable drives, simply select the 'Display Non-Bootable' located in the upper right of the drive selection dialog.

By default, VFC utilises a method of calculation for CHS values based on reading the MBR and then calculating  $\text{Cylinders} = \text{LBA} / \text{Heads} / \text{Sectors}$ . MIP3 & MIP4 use an alternate method of calculation which may result in a different set of values for the resultant CHS. The MIP calculation can be utilised by un-checking the 'Use MBR Geometry for MIP disks'.

*Albeit MIP may mount the disk correctly and logical drives may be accessed via Windows Explorer, it has been noted that the default MIP calculation may cause the subsequent VFC generated VM to fail to boot. Using the MBR method, the same machine will successfully start.*

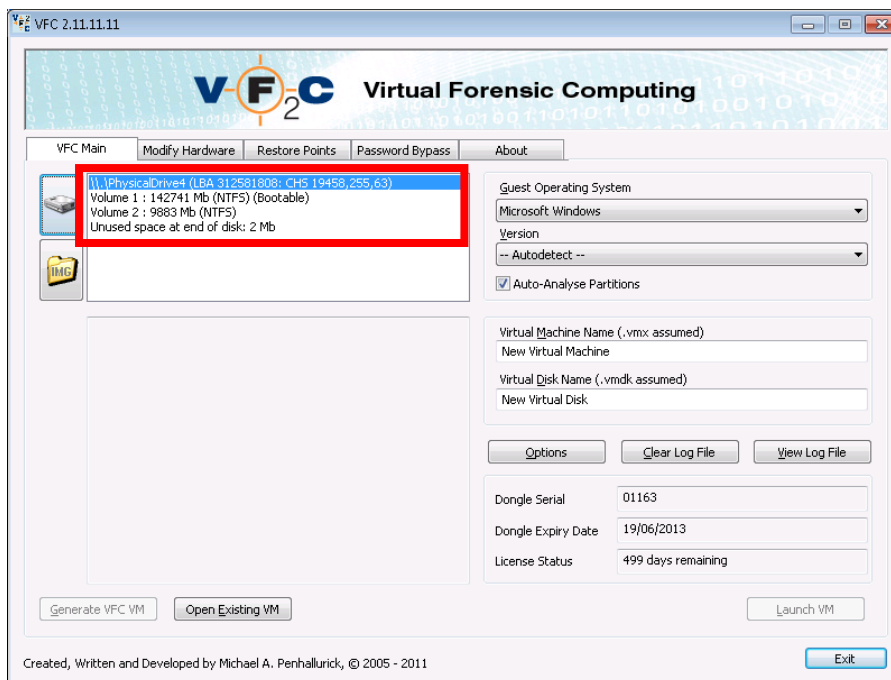
## View Sectors

The 'View Sectors' option enables the user to quickly examine the disk contents in read-only hex-format. There are options available to quickly navigate to the first sector of the disk, the first sector of any identified partitions or to any selected sector on the disk.



## Select Partition

Once the required physical drive has been selected, the available partitions (along with capacity, file system and status) will be displayed on the main dialog screen.



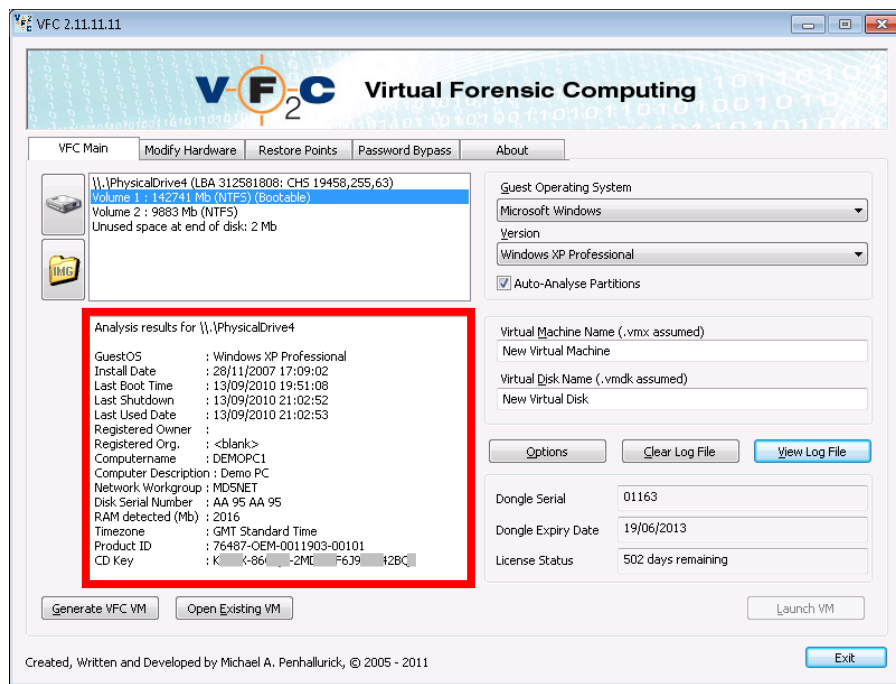
You will now need to select the appropriate 'boot' partition. The boot partition will typically be the partition marked '(Bootable)', but it should be noted that on systems such as Windows Vista and above, the boot partition may actually be the second volume listed. The same would also be true for multi-boot systems, where the OS required to be VFC'd is on a different partition than the boot code for the drive.

If the 'Auto-Analyse Partitions' check box is selected, selecting any of the available partitions will lead to an attempt to auto-detect the installed Windows OS version. This analysis will also try to extract relevant information relating to the installed Windows OS version, which will then be displayed in the lower-left section of the main dialog.

The 'Auto-Analyse Partitions' feature can be disabled if required and the OS version can be manually selected.

*By disabling 'Auto-Analyse Partitions', this will preclude the extraction of any of the aforementioned system information.*

If required, various options which affect the generation of the Virtual Machine can also be altered as desired (see Options, below).

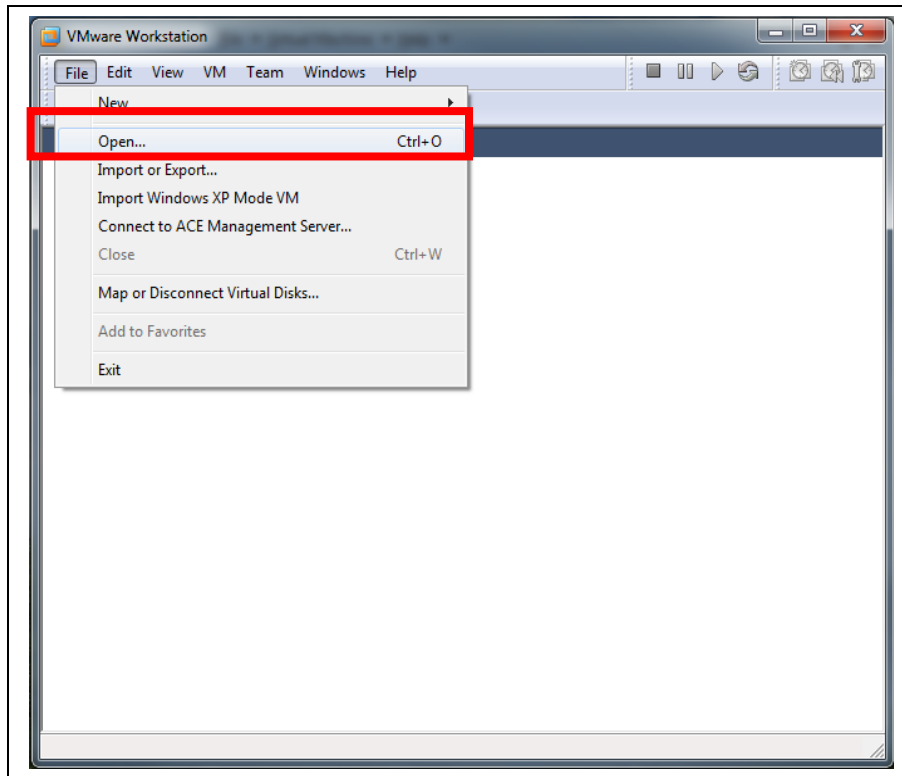


Once the analysis has been completed, you have the option of changing the Virtual Machine Name (default 'New Virtual Machine') and the Virtual Disk Name (default 'New Virtual Disk'). These values should be typically adjusted to reflect the details of the forensic image under investigation (e.g. Coakley-PC, HDD0).

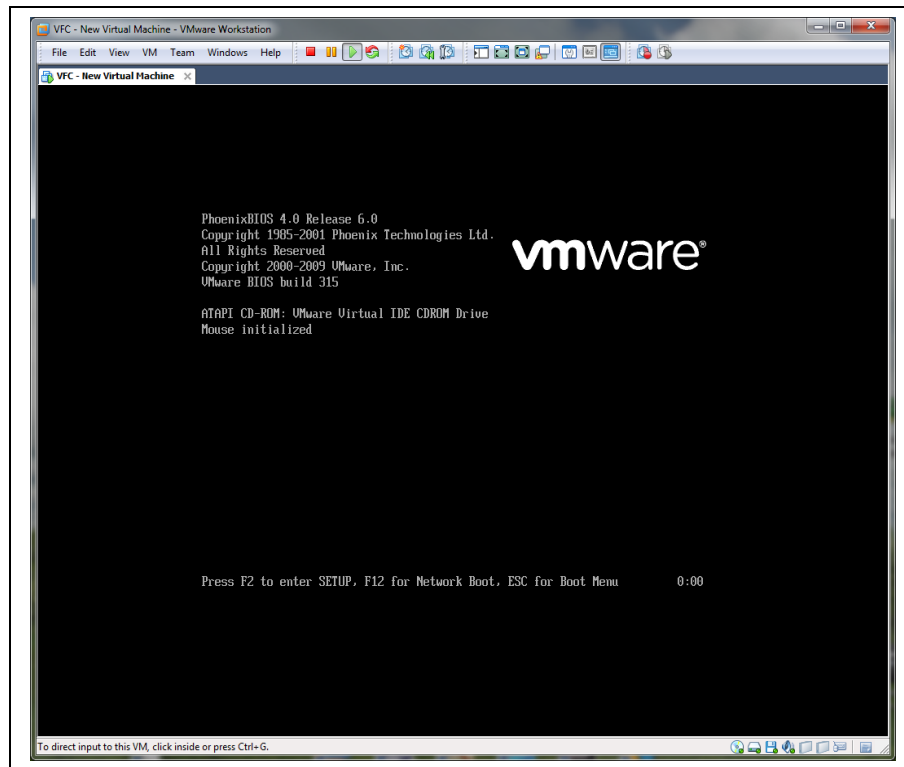
When all relevant data has been entered and analysed, the 'Generate VFC VM' button will become active and the requisite files can be created, along with the application of any necessary system patches.

A successful generation will result in the creation of those files necessary to enable the subject mounted disk image to be booted in a VMware virtual environment. This can be achieved by using the 'Launch' button located at the lower right of the main dialog screen.

Alternatively, the machine can be launched manually, typically by either double-clicking the generated .vmx file via Windows Explorer, or by starting the VMware application and using the various options to Open a Virtual Machine.



Once the Virtual Machine has been manually opened, it will be necessary to 'Power On' the virtual machine.



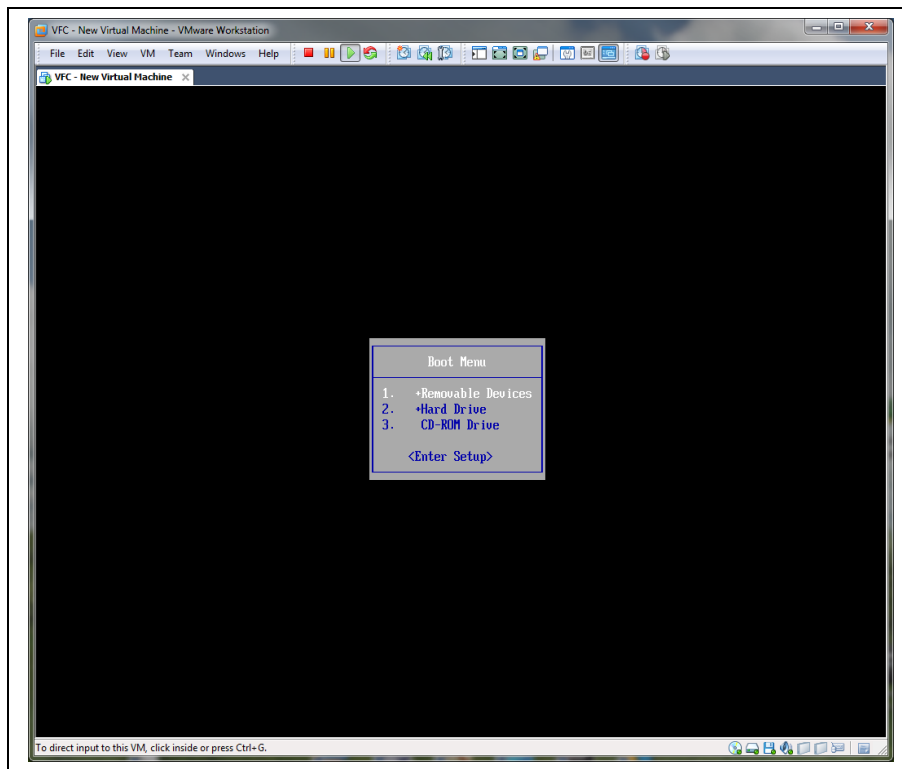
During the boot process, VMware displays options to access Setup (F2), Network Boot (F12) or the Boot Menu (Esc).

By default, VFC does not add any network connectivity.

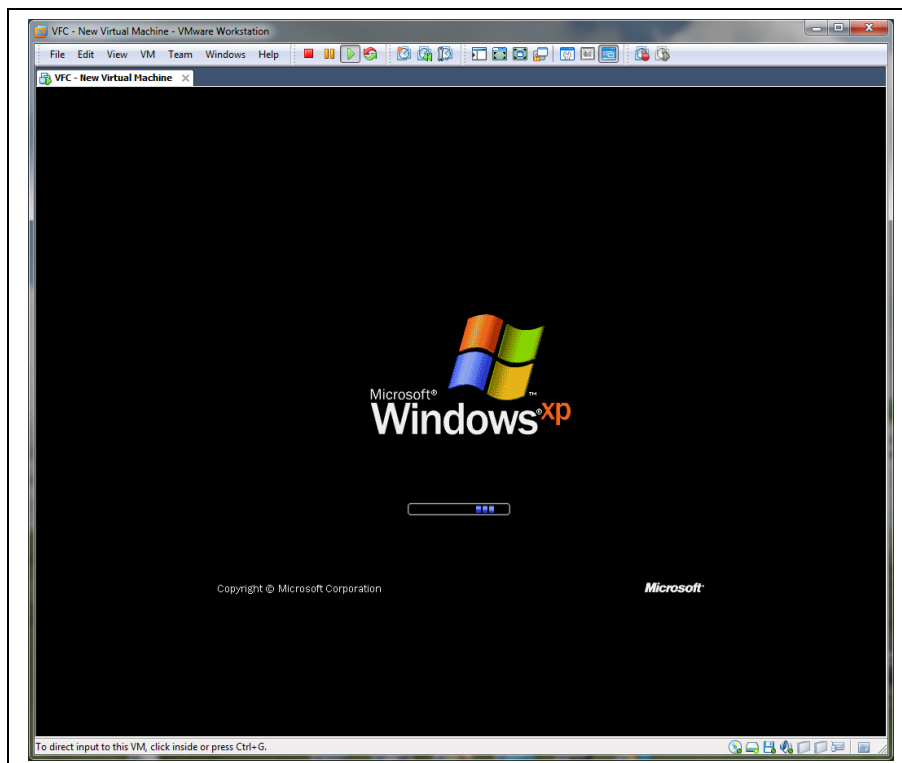
The default boot order is Floppy Disk, Hard Disk then CD-ROM. Typically the Boot Menu will need to be accessed in circumstances whereby the user wishes to boot from a CD or an attached ISO image.

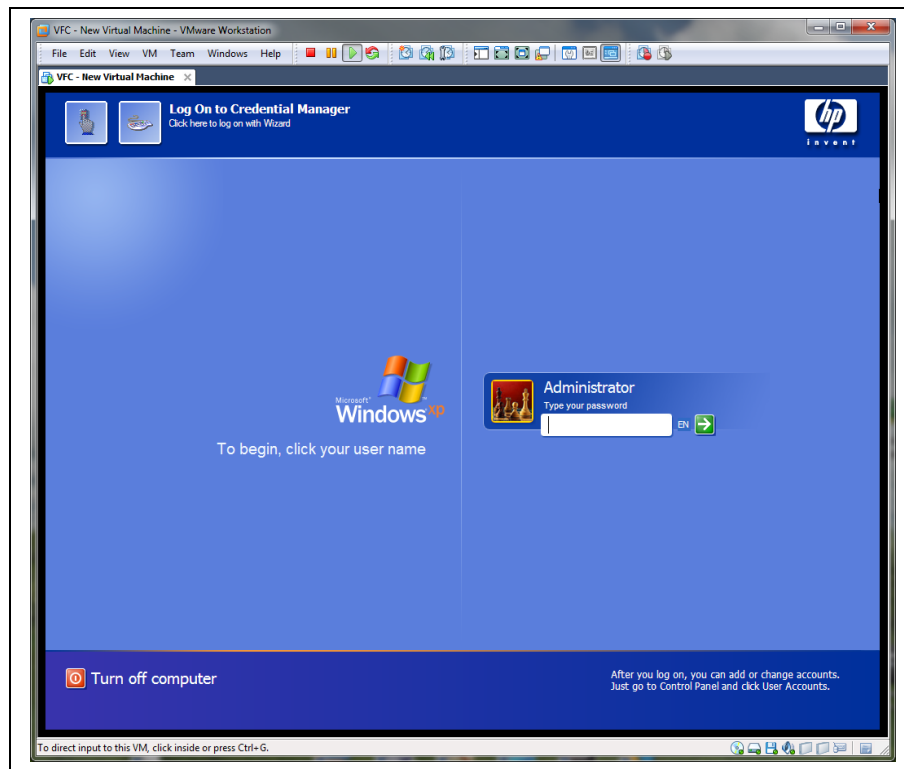
In order to access any of the boot options via the available boot keys, it is first necessary to give focus to the VMware application. Once you power on the virtual machine, move the mouse to a point inside the VMware boot screen and left-click until the mouse cursor disappears. At this point, access to the virtual keyboard will be enabled and pressing the 'Esc' key will display the Boot Menu.

VFC will set the boot delay to 3 seconds (3000 milliseconds) to allow easier access to the boot menu. This value can be manually increased further by editing the generated .vmx file and adjusting the value for 'bios.bootDelay'. To allow a 10 second delay, set this value to '10000'.



Once the desired boot option has been selected (or automatically if the boot menu is not accessed) the boot process will continue and either the logon screen will be displayed or, if the user account has not been password protected, the desktop will be displayed.



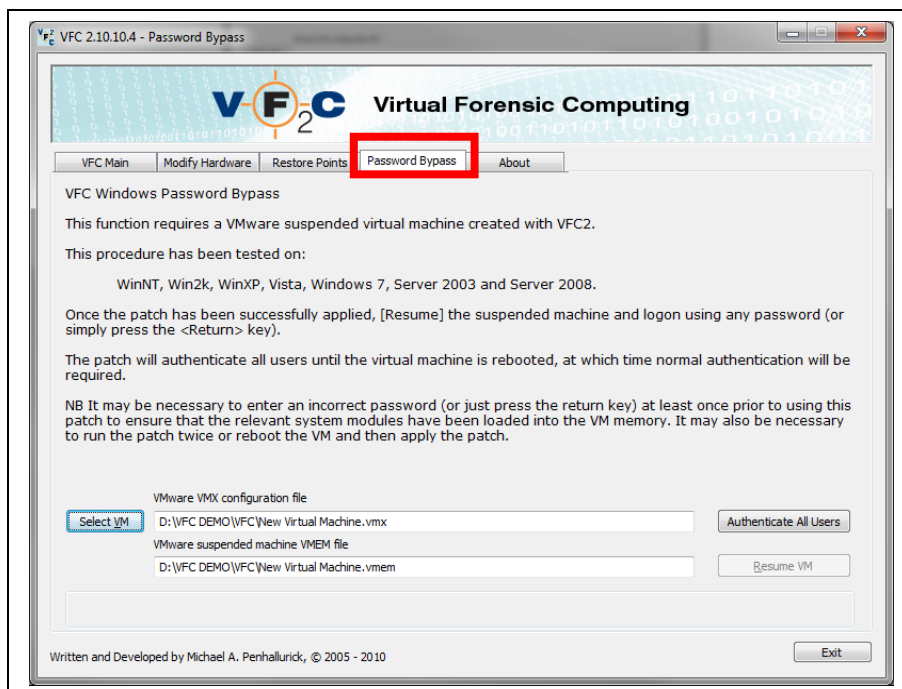


If the user account is password protected, it is possible (on Windows NT & above) to bypass the logon password by utilising the Password Bypass feature.



## Password Bypass

VFC incorporates an innovative method of access to user accounts in a virtual environment with the introduction of Password Bypass. Simply suspend the virtual machine when at the logon prompt, use VFC to select the required .vmx file and then 'Authenticate All Users'.



Once the authentication routine is completed, 'Resume' the virtual machine and access the user account without the need of a password.

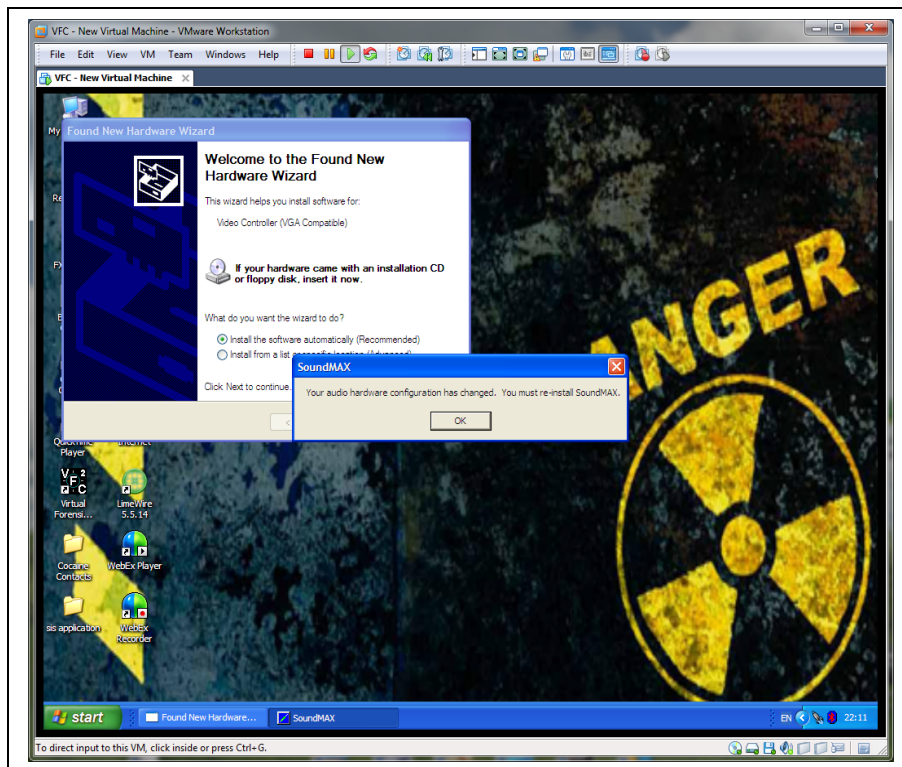
It should be noted that Password Bypass is not a password removal or cracking tool. It is a proprietary routine which works on a single suspended virtual machine session for machines generated by VFC. If the virtual machine is rebooted, memory will be reset and either the password must be utilised or the Password Bypass must be re-applied. No disk files are altered and the effect is transitory.

Additionally, Password Bypass will affect all user accounts on the system, whether they are local user accounts or domain user accounts. When Password Bypass has been applied, access will be available to any relevant user profile present on the system.

*On occasion, VFC may be unable to successfully patch the virtual memory to enable a password bypass. In these instances, VFC can extract relevant system information which is encrypted into a VFC2.PWB file for return to the author such that additional research can be undertaken. No user identifiable information is stored within the PWB file.*

Once you have successfully accessed the desired account, the installed OS will begin to identify new hardware that is detected as a result of the transition to a virtual environment as well as identifying that expected hardware is no longer available.

You will most likely experience a number of message boxes indicating that driver files are being updated/installed. It is likely that certain drivers may not be immediately available, such as the Video Controller (VGA Compatible). Some drivers will become available after the installation of the VMware Tools package, others (e.g. Sound on Windows Vista) may require additional manual intervention.

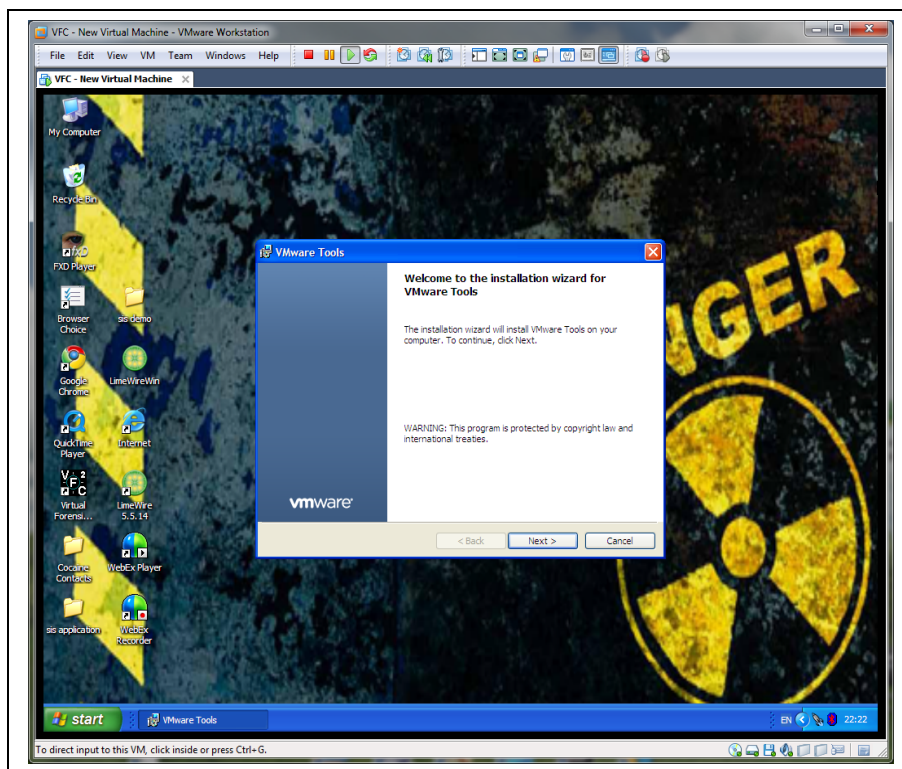


## VMware Tools Installation

A typical installation of VMware Tools will provide enhanced graphic control by utilising the VMware SVGA driver as well as better mouse control and the ability to drag and drop between Host and Guest and vice versa.

Whilst the installation of the VMware Tools is described as vital by VMware (and indeed is required for both enhanced user interaction and to most accurately re-create the original environment), it should be noted that the installation procedure will most likely generate a System Restore Point event.

Equally, if rewinding the machine to an earlier point using System Restore functionality, this will effectively remove the installed Tools from the system and they will need to be installed again.



Once the VMware Tools are installed, it is necessary to restart the machine for configuration changes to take effect.

*During the reboot process after installation of the VMware Tools, the screen resolution may be affected and desktop icons may be re-arranged. It may be possible to adjust screen resolution to the desired final setting prior to the installation of the VMware Tools using the options available within VFC (Currently applicable to Windows XP only). Pre-adjusting resolution may avoid unwanted desktop icon relocation.*

Upon successful reboot (and password bypass if required), you will likely notice a VM tray icon in the lower right of the screen. This can (and probably should) be disabled as it has no direct effect on user data and this icon would NOT be present on an original machine.



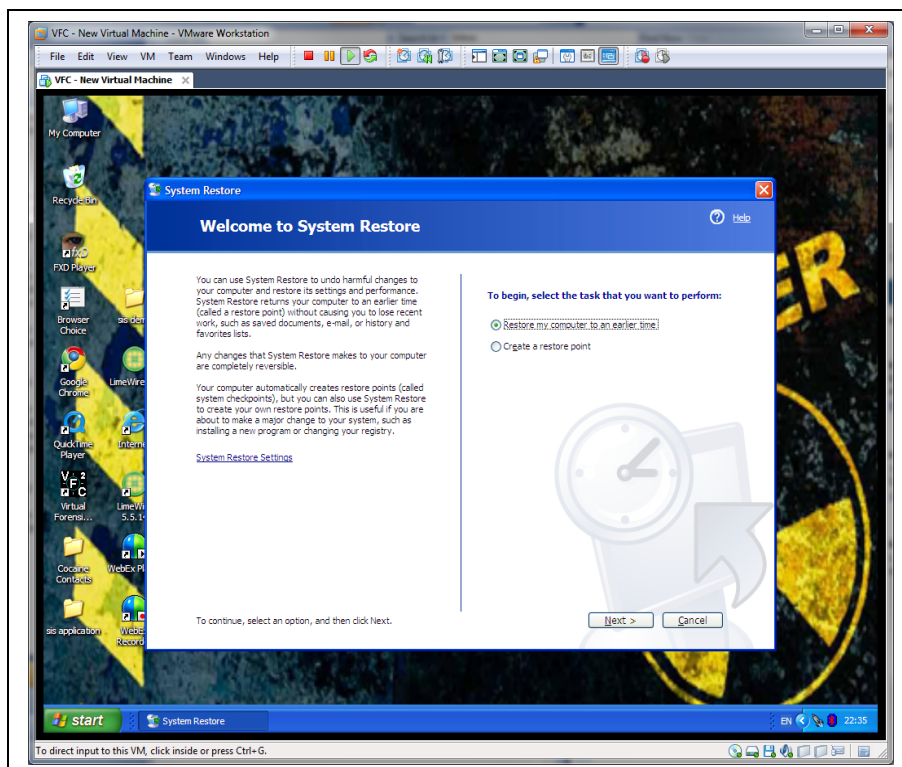
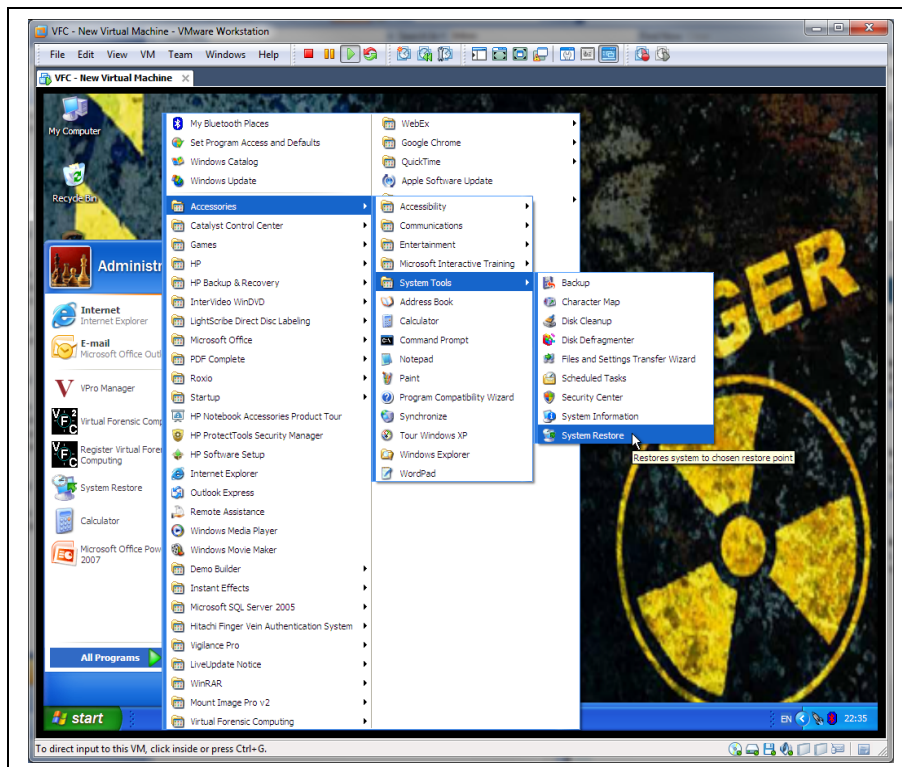
Detailed information about VMware Tools is available within the VMware Workstation User's Manual on the VMware web-site.

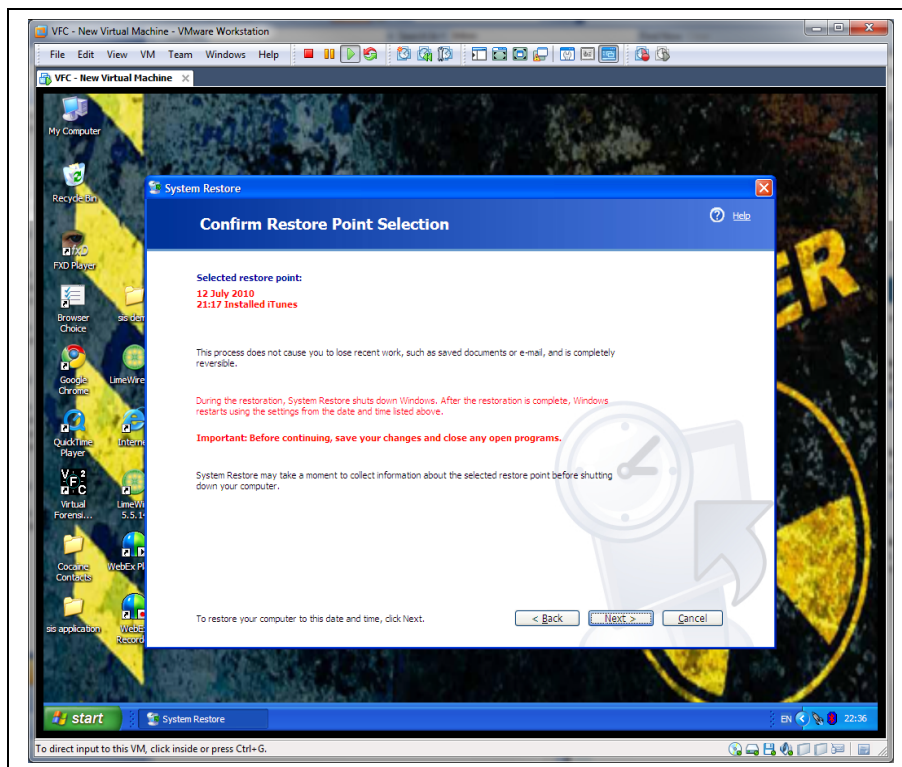
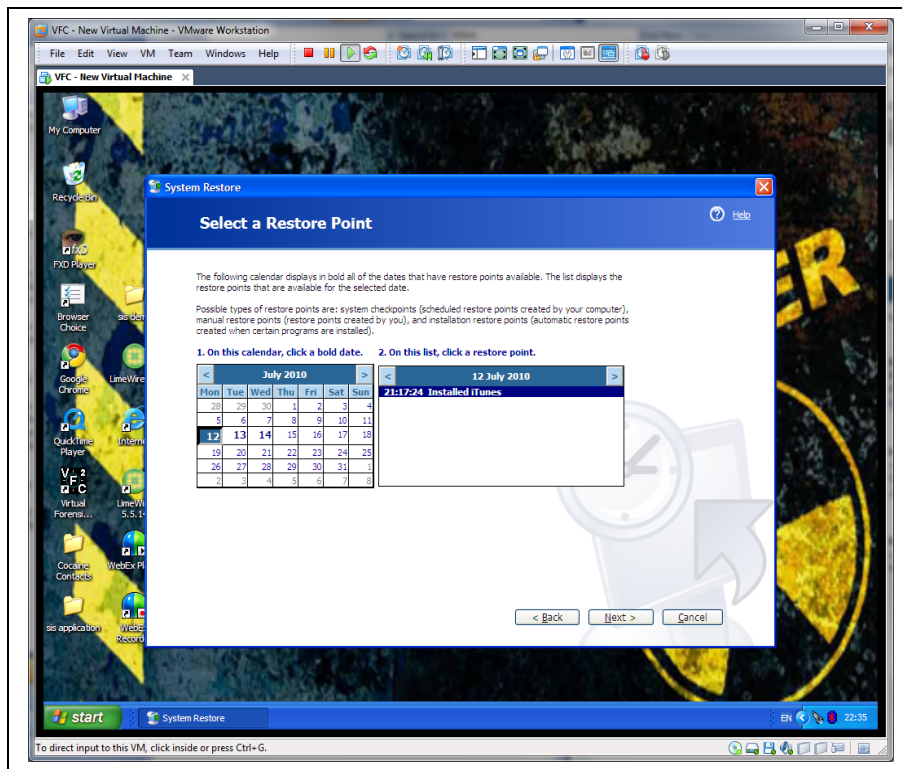
(<http://www.vmware.com/pdf/ws80-using.pdf>)



## System Restore

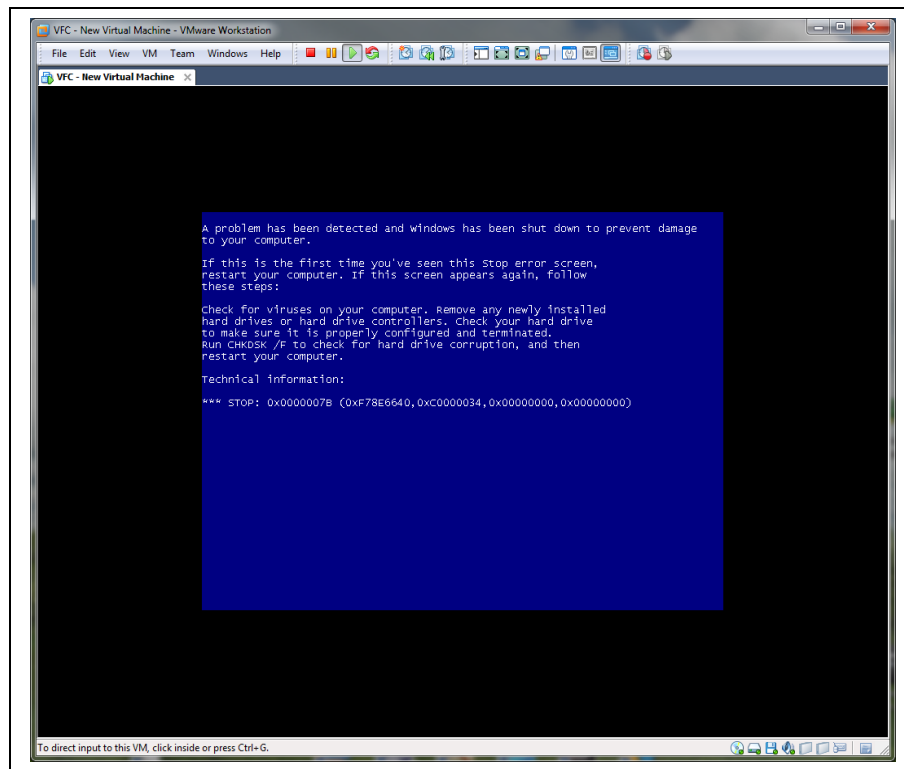
It is possible to utilise the in-built System Restore functionality of Windows XP and above to revert a machine to an earlier state.



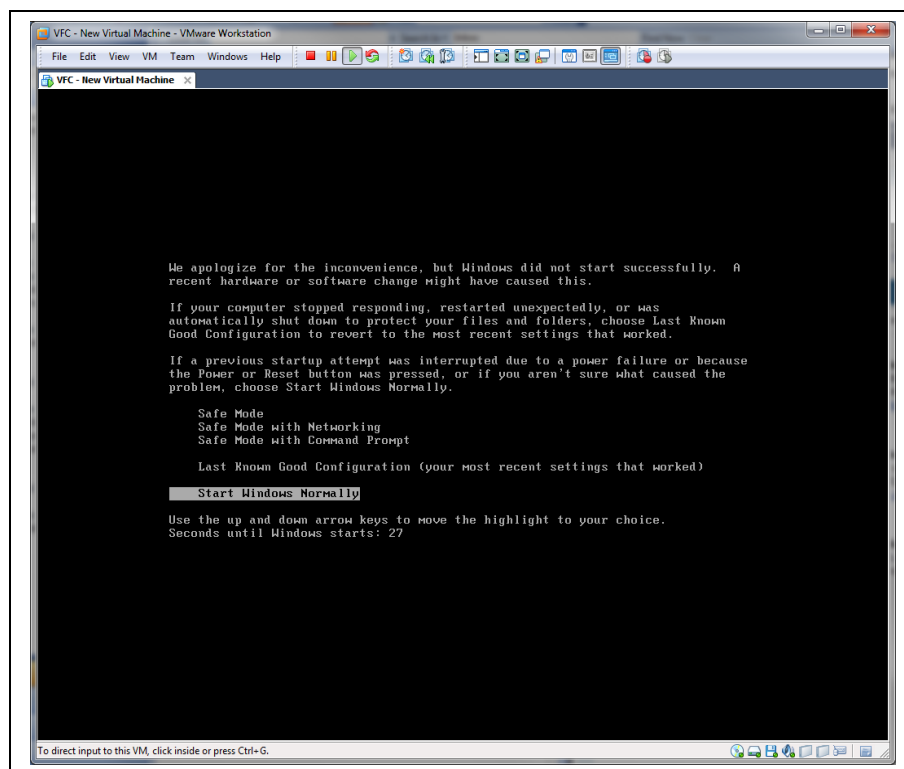


When utilising this functionality, any changes made to the system by VFC and any subsequently installed applications (such as VMware Tools) will be removed.

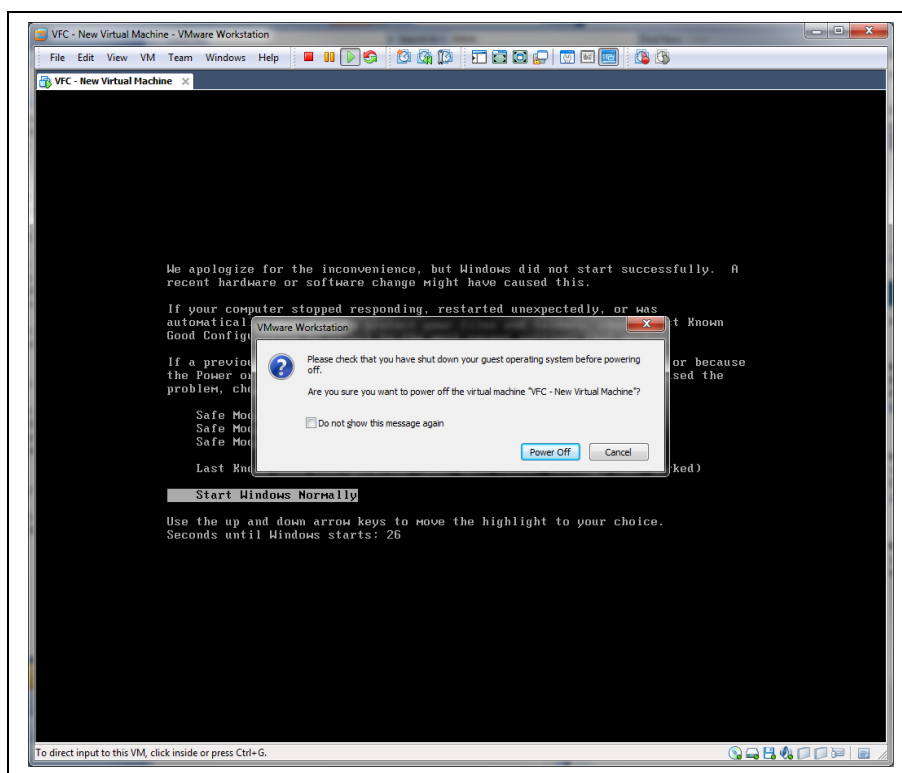
Undoing the VFC changes will cause a 0x7b BSOD (Blue Screen of Death) part way through the process. This is expected behaviour.



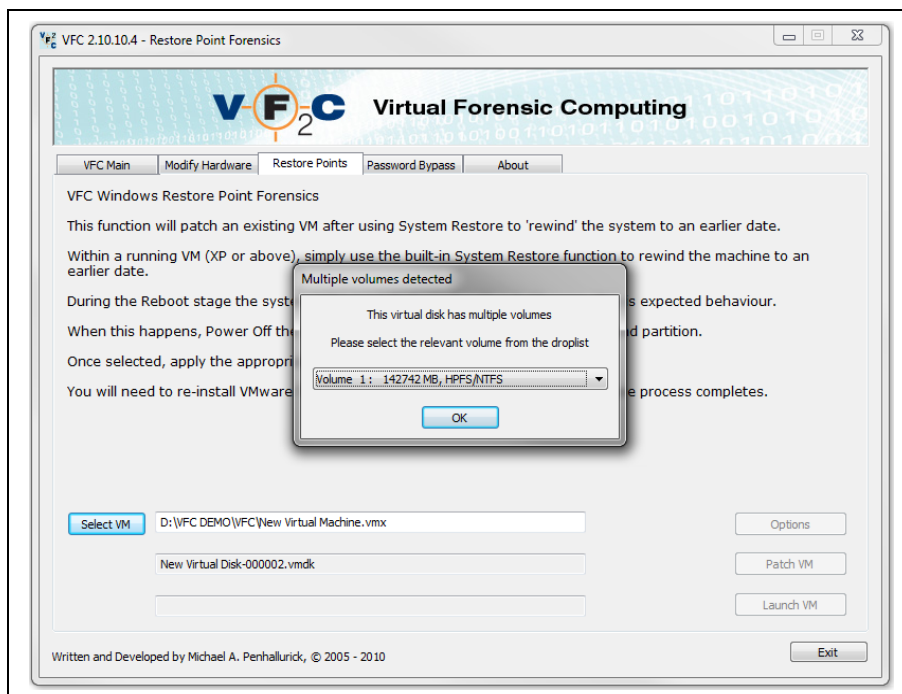
When the system crashes, it will likely go into a cyclical reboot.



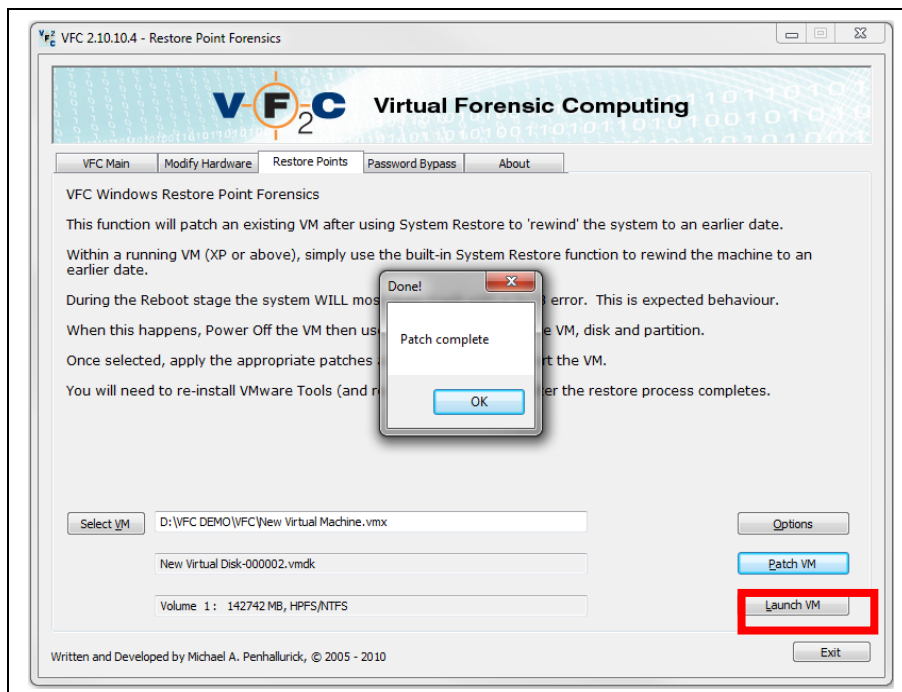
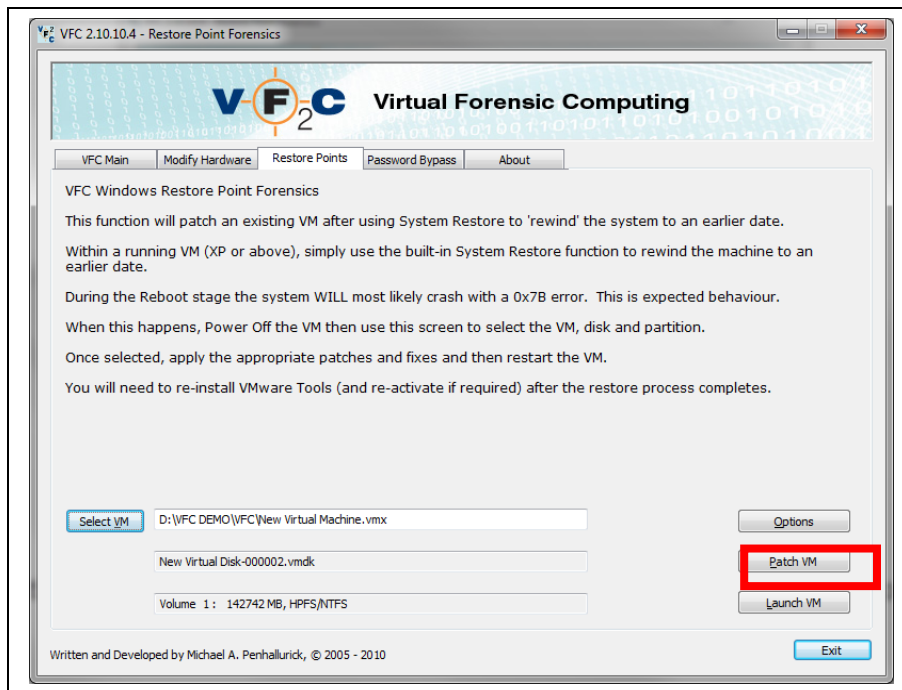
Power off and close (rather than suspend) the Virtual Machine.



Once the VFC VM has been shutdown, utilise the Restore Points tab in VFC to re-inject required system drivers and registry settings.



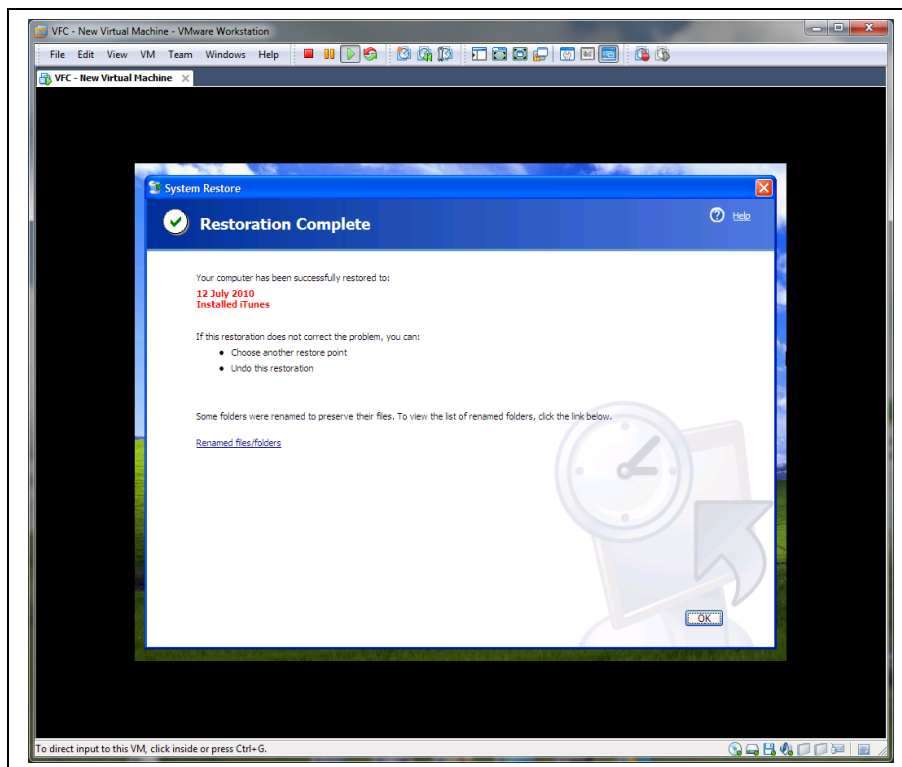
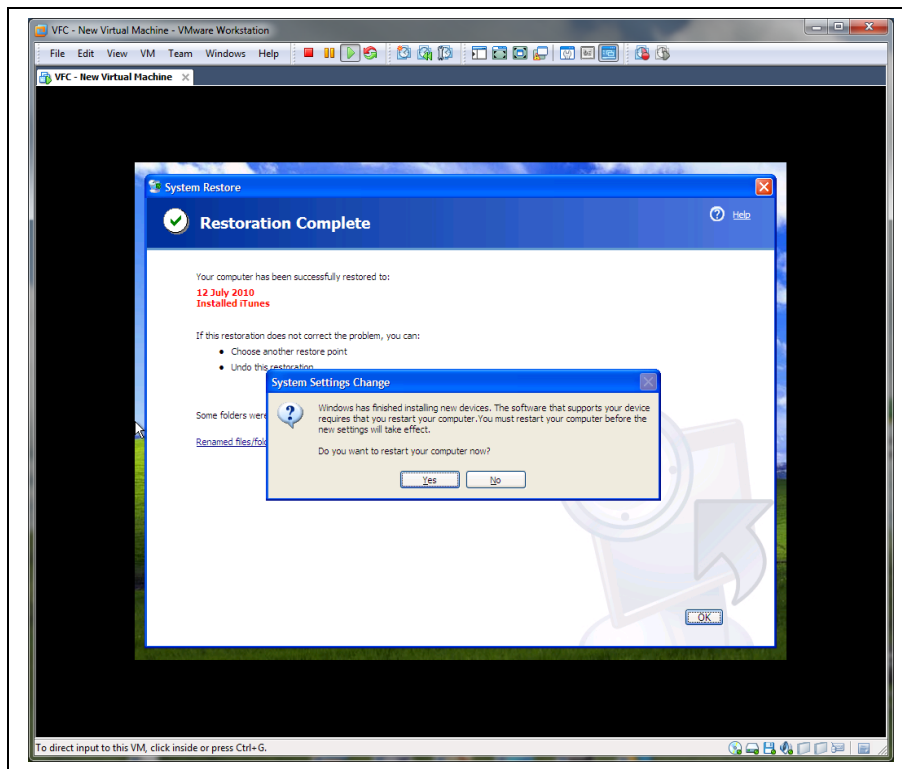




When the machine has been 'patched' you can launch the Virtual Machine and continue the restoration process.

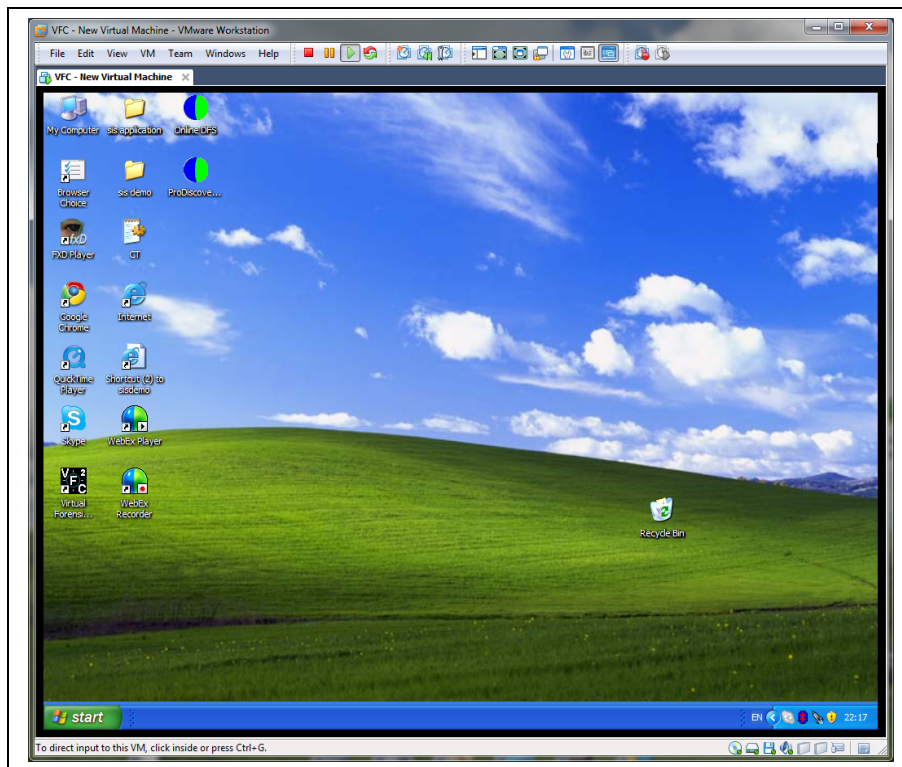
NB A full restoration to an available restore point may take some considerable time.

When the system completes its boot sequence you may again experience alert messages relating to hardware devices, including requests to restart the computer for new devices to take effect.





**Before System Restore on 13 September 2010**



**After System Restore Point of 12 July 2010**

## **Creating a standalone Virtual Machine from a VFC VM**

On occasion it may be necessary to create a standalone copy of a VFC VM for a client whom does not have access to mounting utilities such as MIP or the main VFC program.

NB When using the following methods to create a copy VFC VM, unless snapshots are carefully used, the forensic integrity of the methodology will be compromised as the standalone machine cannot be readily recreated and returned to its initial state.

### *Standalone VFC VM using a DD image*

The most direct way of creating a standalone VFC VM which can be run within the VMware platform without further requirement of the VFC application or any third part forensic image mounting utilities is simply by using raw 'dd' images as the source device rather than a physical drive (mounted or real).

Since no mounting utilities have been employed, the resultant VFC VM files, along with the original 'dd' images, can be transferred to any suitably large enough storage device. The only requirement will be that the client has access to at least VMware Player in order to open the relevant .vmx file and launch the virtual machine.

It should be noted that advanced features available from VFC such as Password Bypass will not be available and as such the appropriate logon credentials will be required or alternate means will be necessary in order to obviate this requirement.

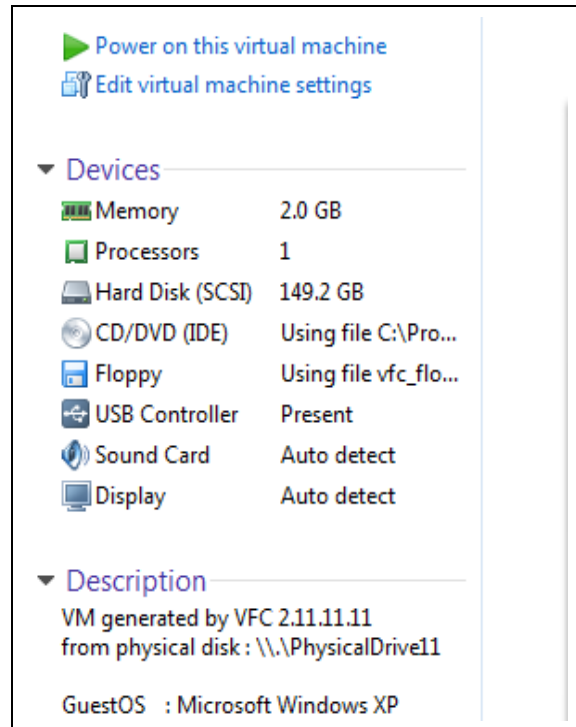
### *Duplicate VFC VM using disk-copy method*

A legacy process initially used during the development of The VFC Method is the utilisation of a third party disk cloning application, such as Norton Ghost or the freely available Clonezilla, in order to create a full disk copy of the live data of the subject system. This copy can be subsequently 'preserved and protected' by using snapshots such that the resultant VM can be successfully reverted to it's initial VFC state if required.

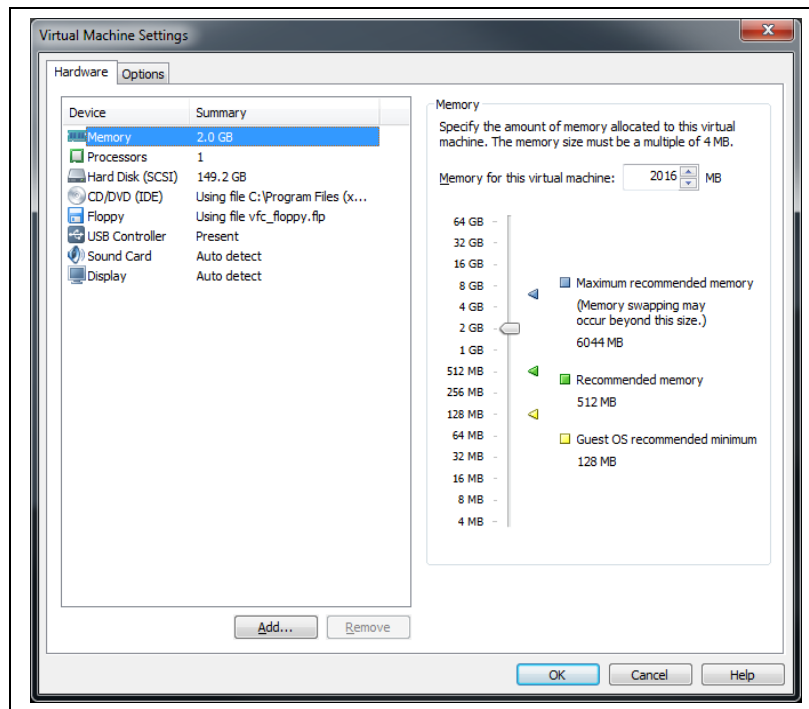
By using a disk cloning application and utilising the sparse disk feature of VMware vmrk files, the actual disk space used is, or can be, considerably smaller than the original disk capacity as only 'live' data is selected for copying. Deleted files and unallocated disk space are ignored, resulting in a much smaller yet still accurate representation of the user system as all relevant system and user files (including those in the Recycle Bin) are available.

The downside of this method is that it can be a quite time-consuming process to copy the disk data; however, in those instances where a generated VFC VM is required to be run independently of forensic images and access to mounting utilities such as MIP, this method can be implemented.

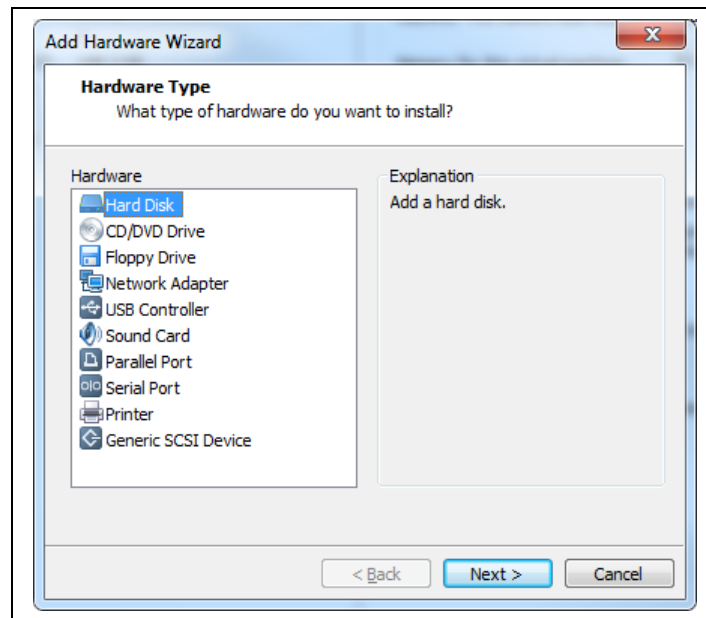
The following screenshots depict the process by which a new, suitably sized 'sparse' disk is created and added to the VFC VM using VMware Workstation 8.



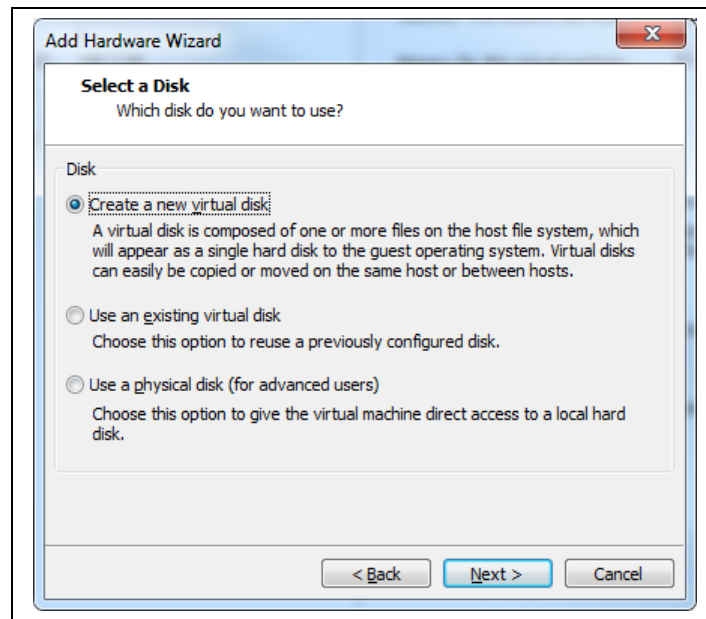
First, select the option to 'Edit virtual machine settings'.



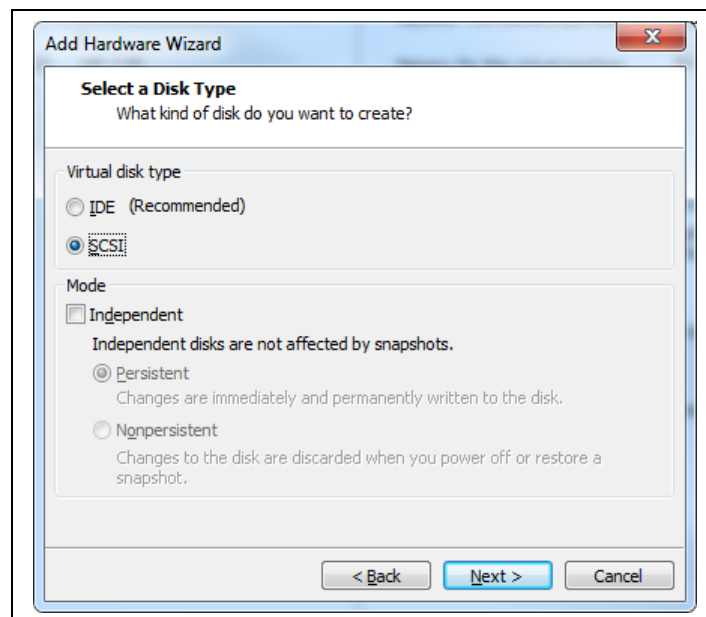
Click 'Add', the 'Add Hardware Wizard' will start and the default option will be for a 'Hard Disk'.



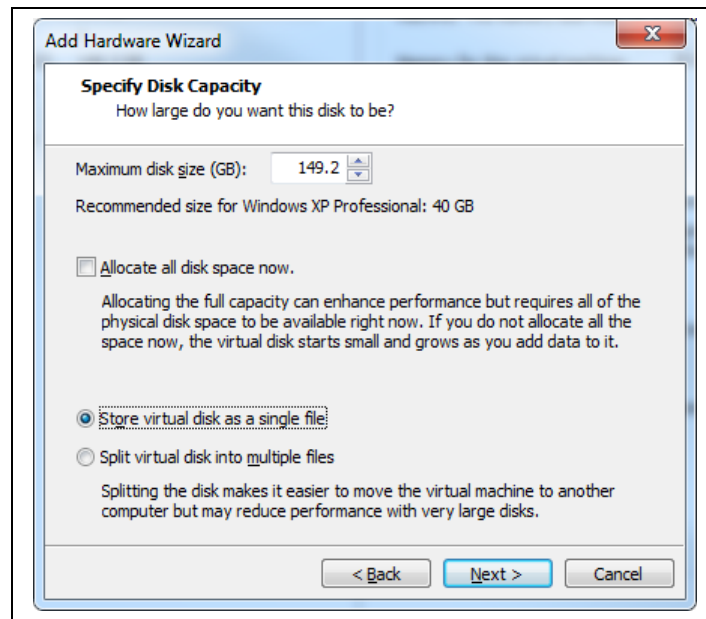
Click 'Next'.



The default option is to 'Create a new virtual disk', so just click 'Next'.



Select the appropriate 'Virtual disk type'; if your VFC VM is using SCSI disks, then select SCSI here. You can ignore the disk mode at this stage.



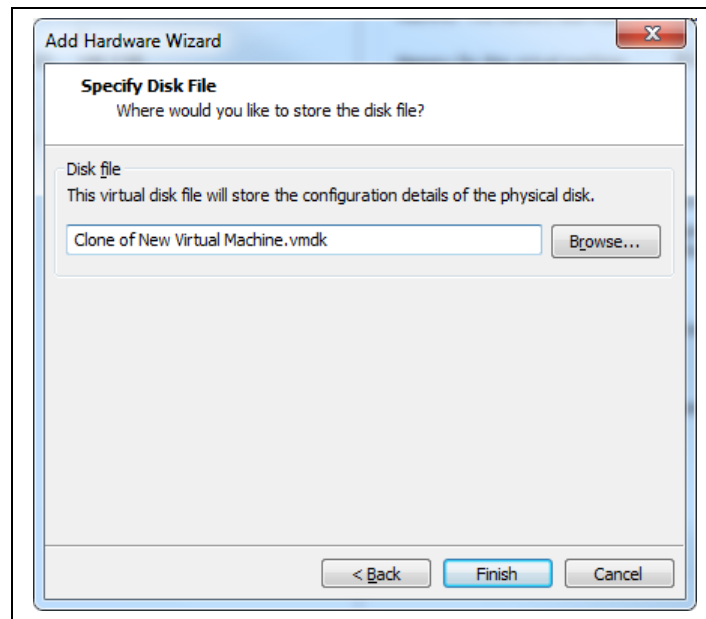
Unlike OEM drive manufacturers, VMware disk sizes are calculated at the true specified capacity. The original hard disk being used in this example was a 160GB disk (149.2GB formatted). When specifying the disk size in VMware, it is usually sufficient to simply specify the formatted disk size as the size of the disk.

In this instance, specify the same capacity as displayed in the initial VFC VM settings screen (above) which is shown as 149.2GB.

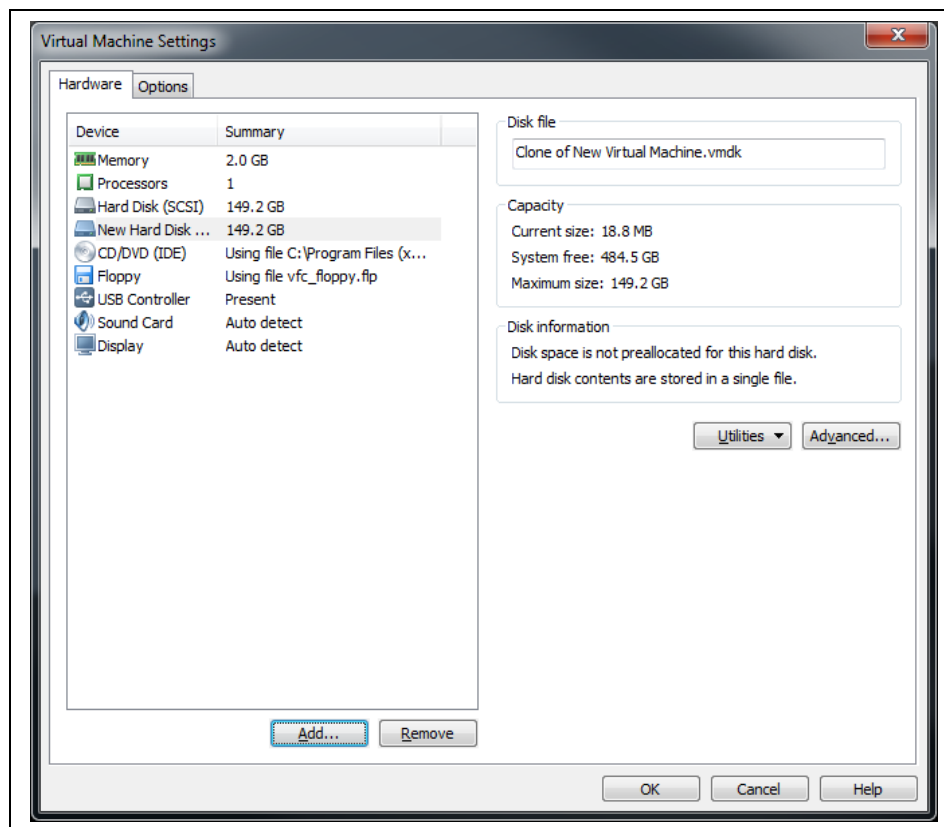
I usually elect to NOT allocate the disk space and to store the disk as a single file.

NB You will need to use a file system (NTFS) which can support large file sizes if storing as a single file. FAT32 drives have a 4GB file size limitation and you will need to 'Split the disk into multiple files' if using a FAT32 storage drive on your Host system.

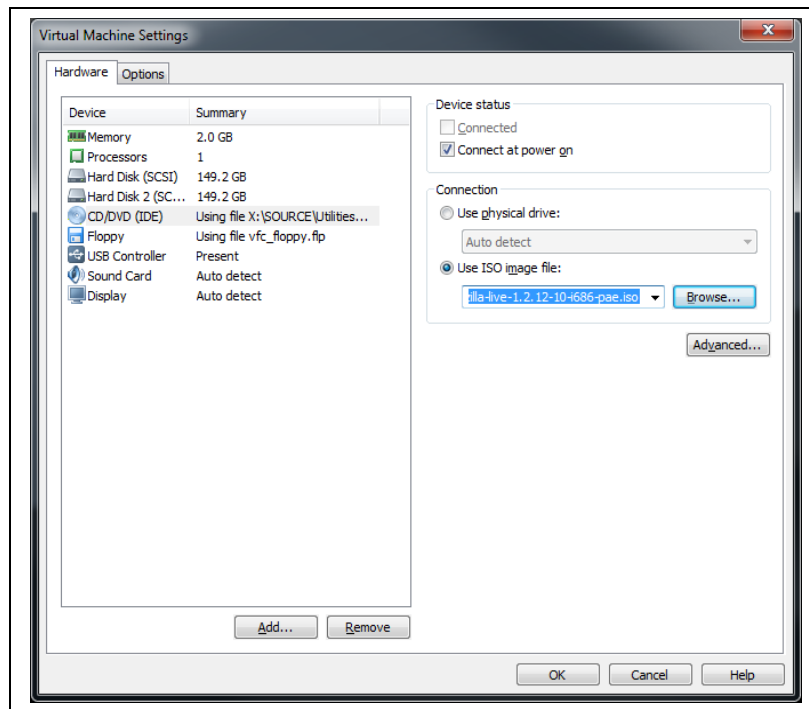




Specify the name of the new disk and click 'Finish'



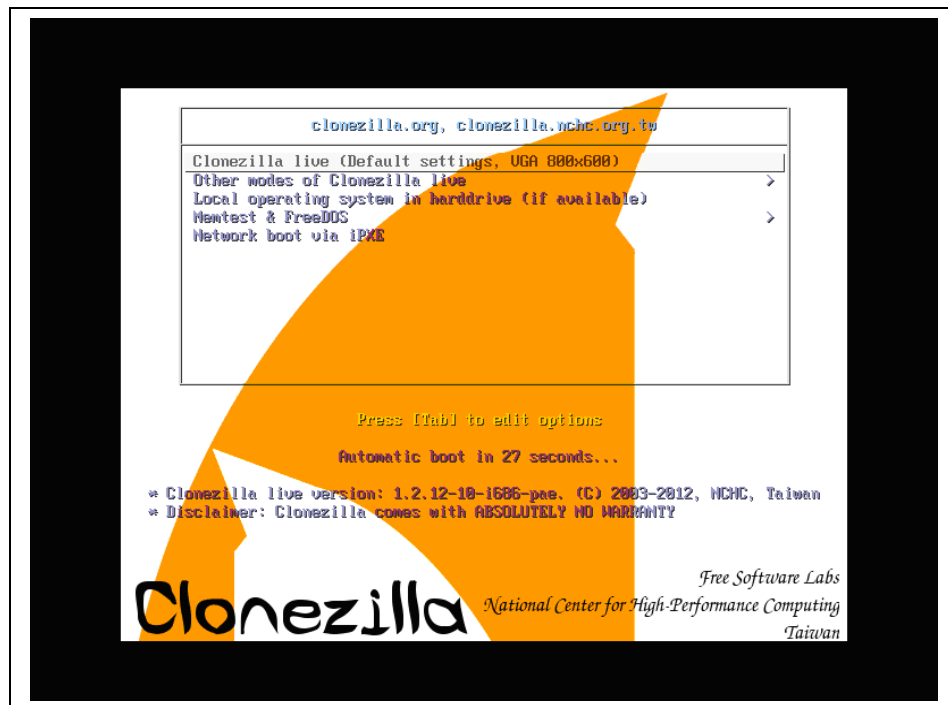
I usually use ISO image files of CD/DVD media rather than physical discs. Click on the CD/DVD entry in the Virtual Machine Settings dialog (it should still be open from adding the disk), select 'Use ISO image file' and navigate to the local host folder where your ISO image is located. In this example I am using *clonezilla-live-1.2.12-10-i686-pae.iso* (available from <http://clonezilla.org/>).



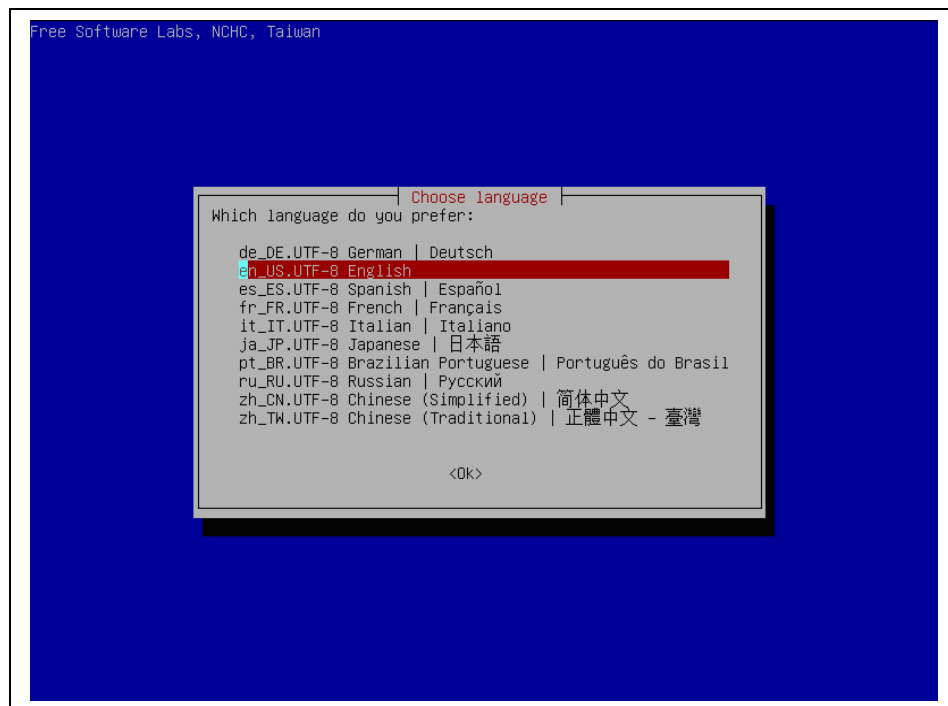
To make the VFC VM boot from CD, simply power on the machine, give the machine focus by using the mouse to click inside the VM and then press the ESC key once. The following Boot Menu will be displayed, simply use the cursor keys to select option '3. CD-ROM Drive' and press Enter.



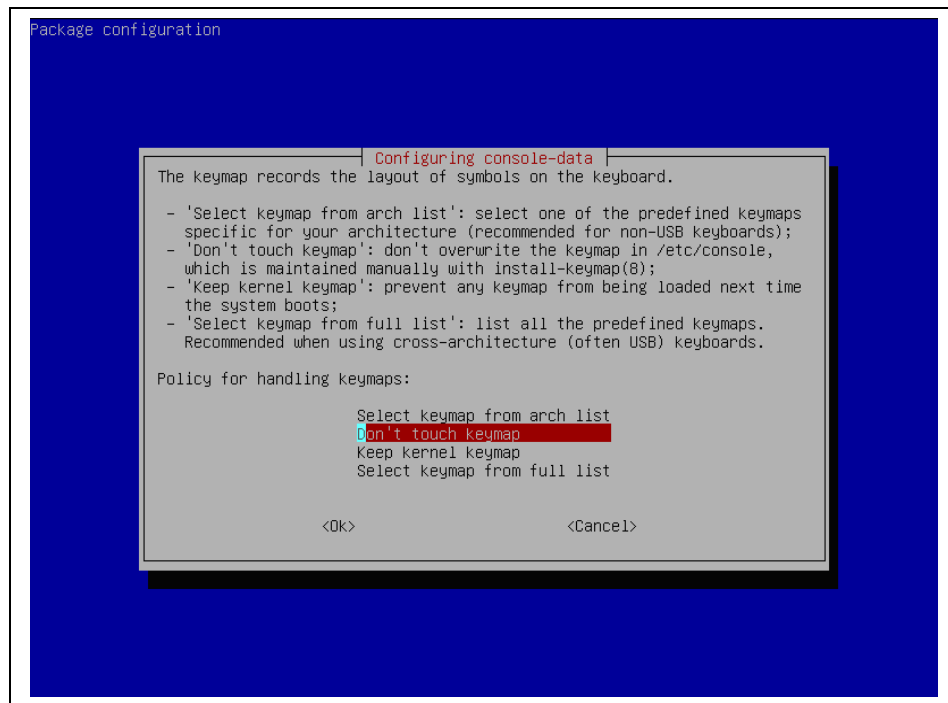
The machine will now boot from your CD-ROM ISO file and you will see the following screen (or similar dependent on the version that is current when you perform these steps).



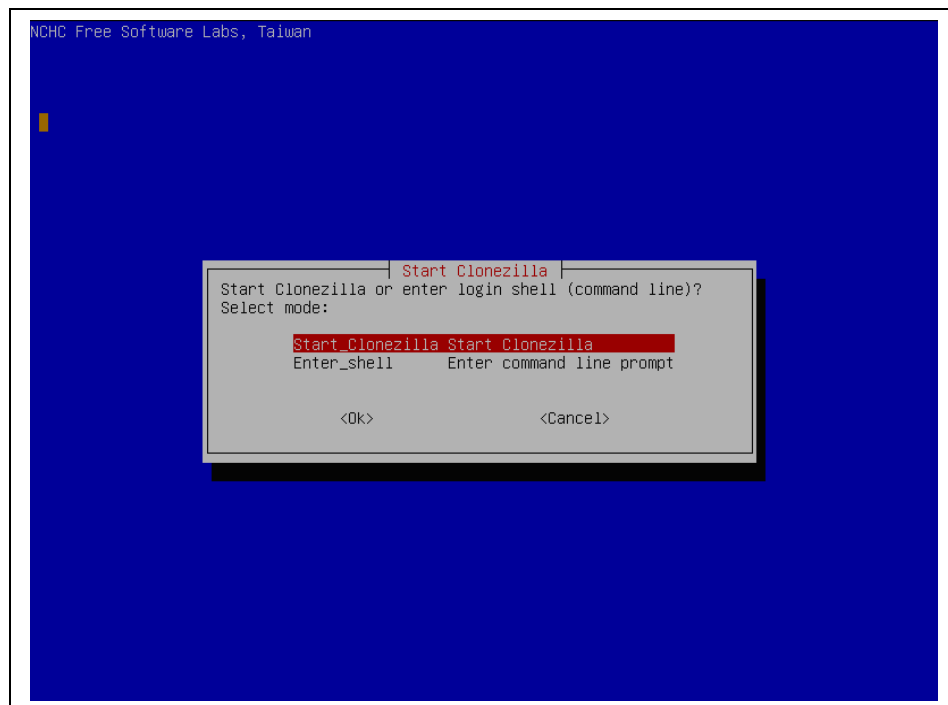
Press 'Enter' to boot with default options or wait for the boot timer to finish.



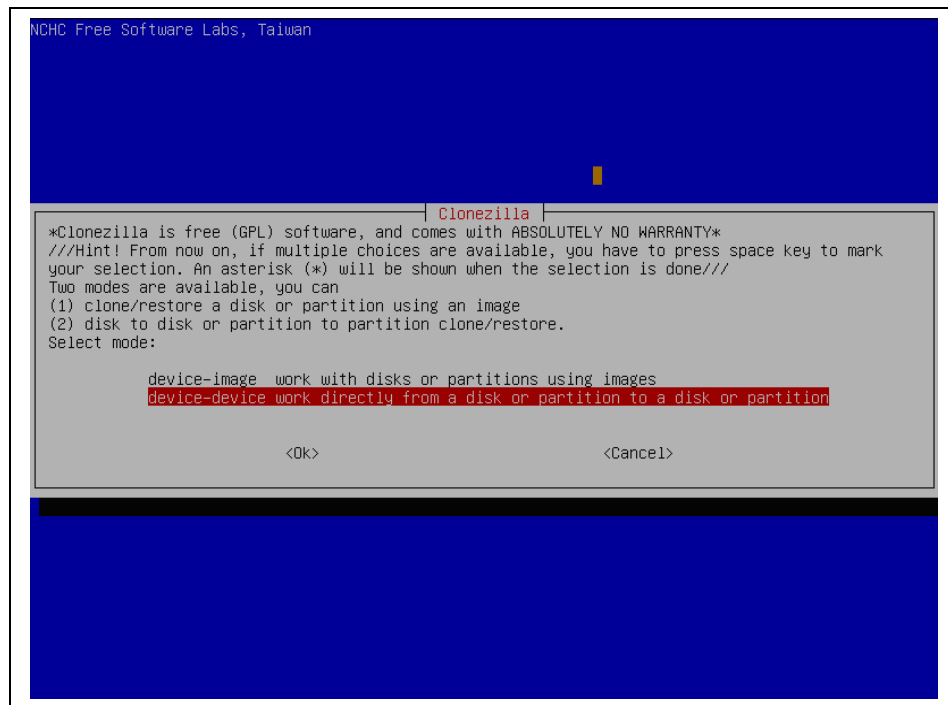
Select the preferred language (default is English).



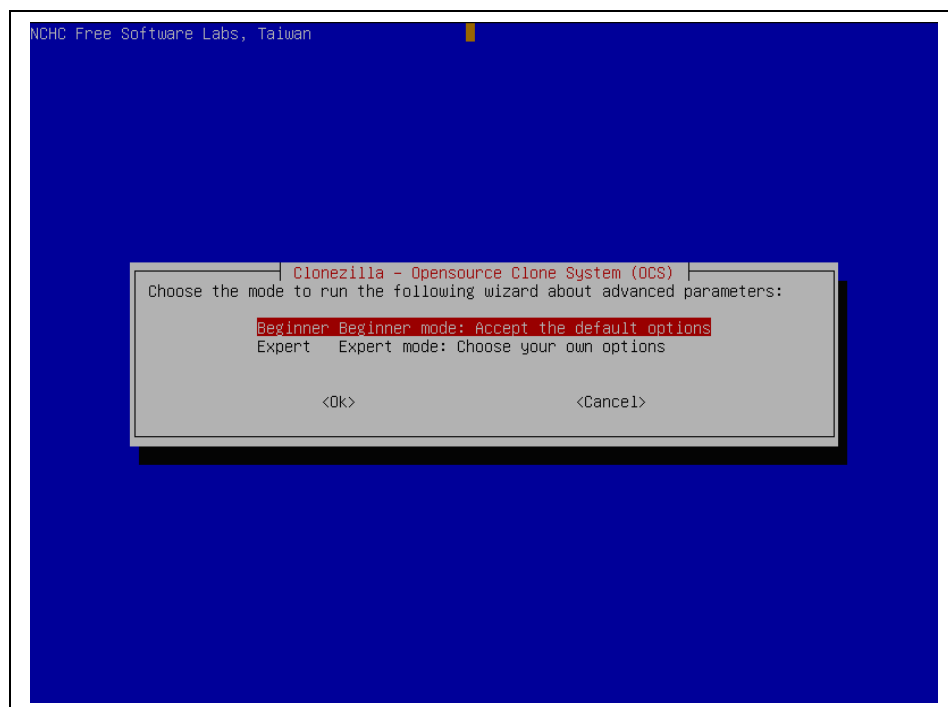
There should be little need to alter the keymap.



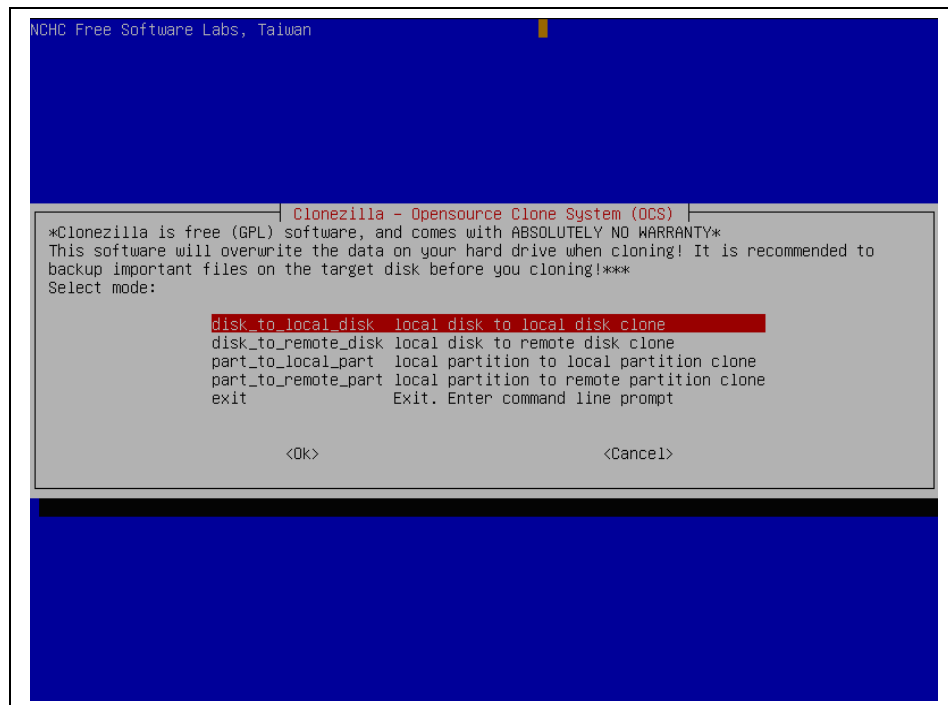
Click 'OK' to start Clonezilla.



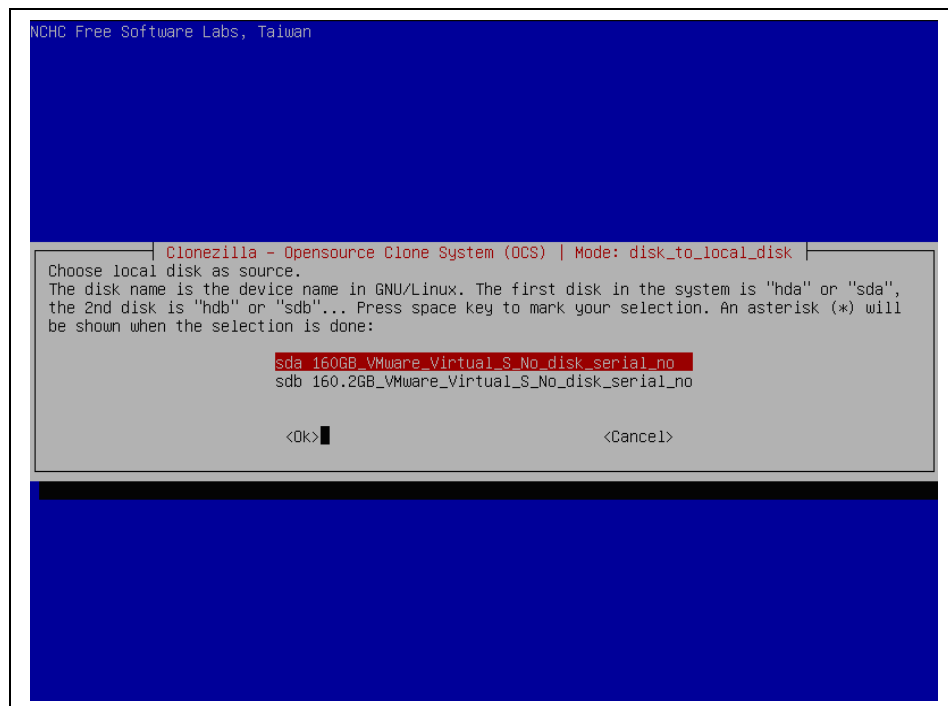
Select 'device-device' option and click 'OK'.



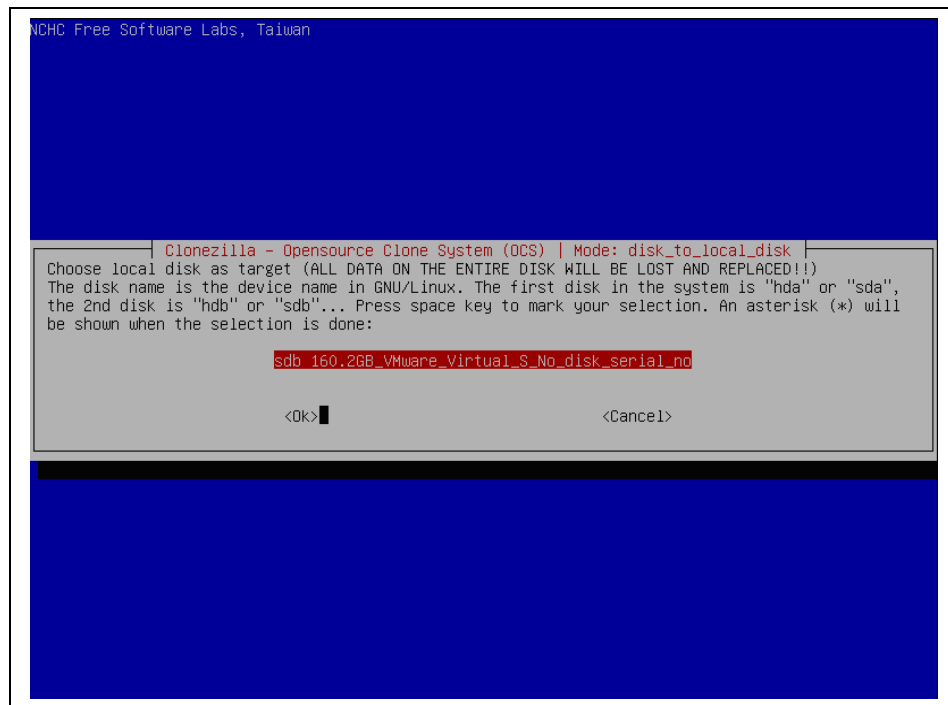
Selecting 'Beginner' mode should suffice for our cloning needs. Click 'OK'.



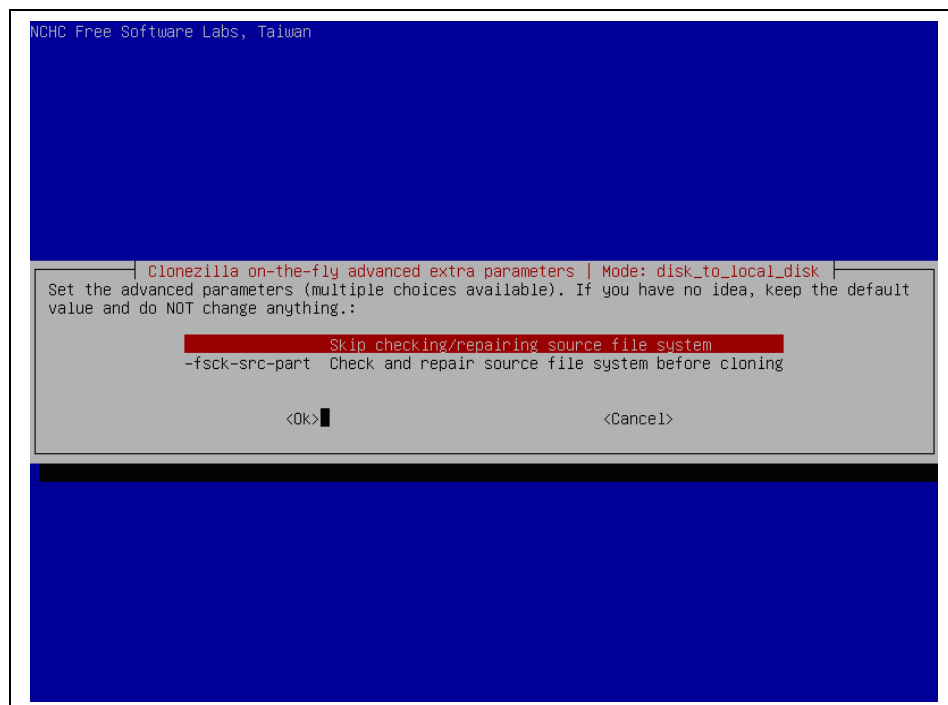
We will be cloning from (virtual) disk to (virtual) local disk. Click 'OK'.



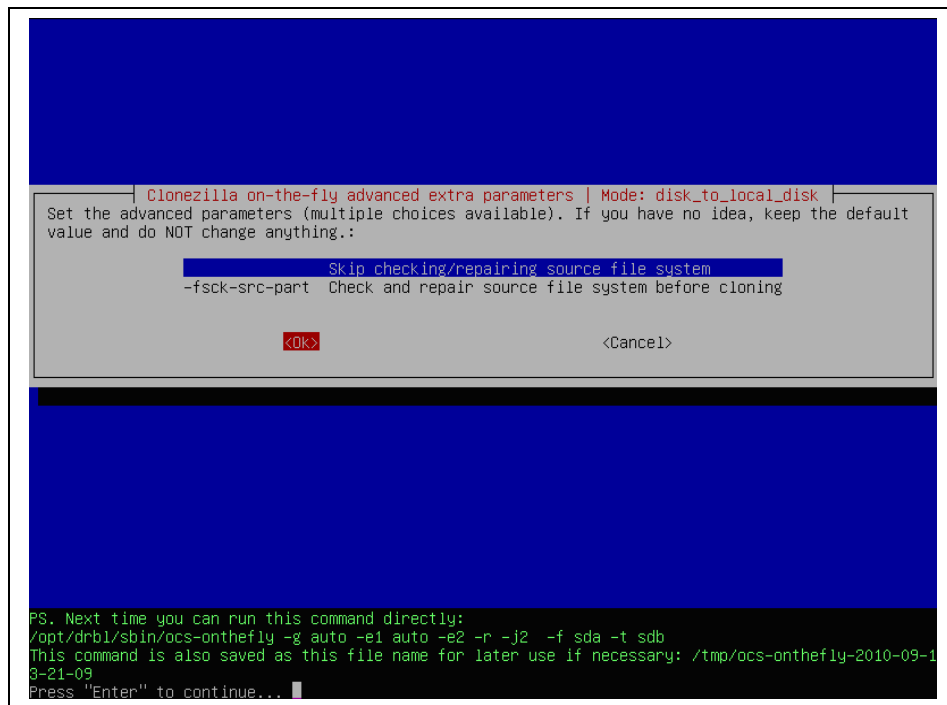
The first drive shown should be our original VFC'd drive. Click 'OK'.



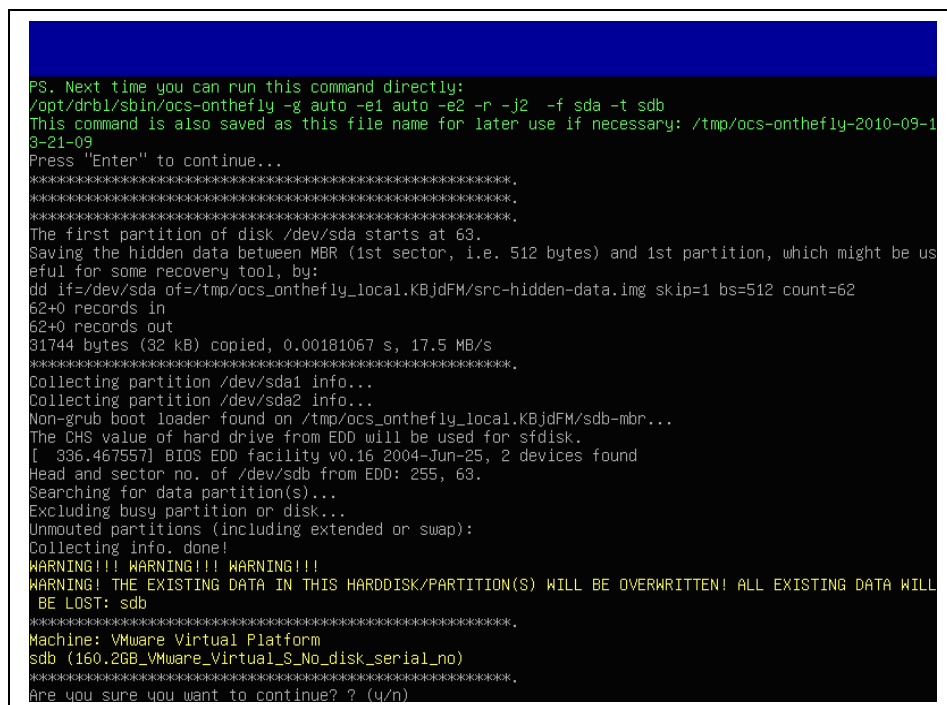
The remaining disk (our blank virtual disk target) will now be displayed. Click 'OK'.



There should not be a need to run any disk check options but if required, these can be selected here. Click 'OK'.



Further confirmation will be required to start the process. Press 'Enter' to continue.



You will be prompted multiple times to make sure you are sure you want to continue. Press 'y' then 'Enter' to continue.



```

Saving the hidden data between MBR (1st sector, i.e. 512 bytes) and 1st partition, which might be useful for some recovery tool, by:
dd if=/dev/sda of=/tmp/ocs_onthefly_local.KBjdFM/src-hidden-data.img skip=1 bs=512 count=62
62+0 records in
62+0 records out
31744 bytes (32 kB) copied, 0.00181067 s, 17.5 MB/s
*****
Collecting partition /dev/sda1 info...
Collecting partition /dev/sda2 info...
Non-grub boot loader found on /tmp/ocs_onthefly_local.KBjdFM/sdb-mbr...
The CHS value of hard drive from EDD will be used for sfdisk.
[ 336.467557] BIOS EDD facility v0.16 2004-Jun-25, 2 devices found
Head and sector no. of /dev/sdb from EDD: 255, 63.
Searching for data partition(s)...
Excluding busy partition or disk...
Unmounted partitions (including extended or swap):
Collecting info. done!
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL BE LOST: sdb
*****
Machine: VMware Virtual Platform
sdb (160.2GB_VMWare_Virtual_S_No_disk_serial_no)
*****
Are you sure you want to continue? ? (y/n) y
OK, let's do it!!
*****
Will create the partition on the target machine...
Let me ask you again.
*****
Machine: VMware Virtual Platform
sdb (160.2GB_VMWare_Virtual_S_No_disk_serial_no)
*****
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL BE LOST: sdb
Are you sure you want to continue? ? (y/n) y

```

In case you change your mind, you can abandon the cloning now. Since we should really know what we are doing, press 'y' then 'Enter' to continue.

```

Units = sectors of 512 bytes, counting from 0

   Device Boot      Start         End      #sectors  Id System
 /dev/sdb1  *           63    292334804    292334742   7  HPFS/NTFS/exFAT
 /dev/sdb2           292334805    312576704    20241900   7  HPFS/NTFS/exFAT
 /dev/sdb3              0           -            0   0  Empty
 /dev/sdb4              0           -            0   0  Empty
Successfully wrote the new partition table

Re-reading the partition table ...
[ 401.203002] sd 1:0:1:0: [sdb] Cache data unavailable
[ 401.203436] sd 1:0:1:0: [sdb] Assuming drive cache: write through
[ 401.203999] sdb: sdb1 sdb2

If you created or changed a DOS partition, /dev/foo7, say, then use dd(1)
to zero the first 512 bytes: dd if=/dev/zero of=/dev/foo7 bs=512 count=1
(See fdisk(8).)
This is done by "sfdisk --force -C 19476 -H 255 -S 63 /dev/sdb < /tmp/ocs_onthefly_local.KBjdFM/tgt_
pt.sf"
Informing the OS that partition table has changed...
[ 401.279799] sd 1:0:1:0: [sdb] Cache data unavailable
[ 401.280630] sd 1:0:1:0: [sdb] Assuming drive cache: write through
[ 401.281165] sdb: sdb1 sdb2
Checking the integrity of partition table in the disk /dev/sdb...
done!
*****
The first partition of disk /dev/sdb starts at 63.
Restoring the hidden data between MBR (1st sector, i.e. 512 bytes) and 1st partition, which might be
useful for some recovery tool, by:
dd if=/tmp/ocs_onthefly_local.KBjdFM/tgt-hidden-data.img of=/dev/sdb seek=1 bs=512 count=62
62+0 records in
62+0 records out
31744 bytes (32 kB) copied, 0.00197847 s, 16.0 MB/s
*****
*****
Do you want to clone the boot loader (executable code area, the first 446 bytes) to: sdb ?
(Y/n)

```

We want the whole image, including the boot loader, so press 'y' then 'Enter' to continue.

```

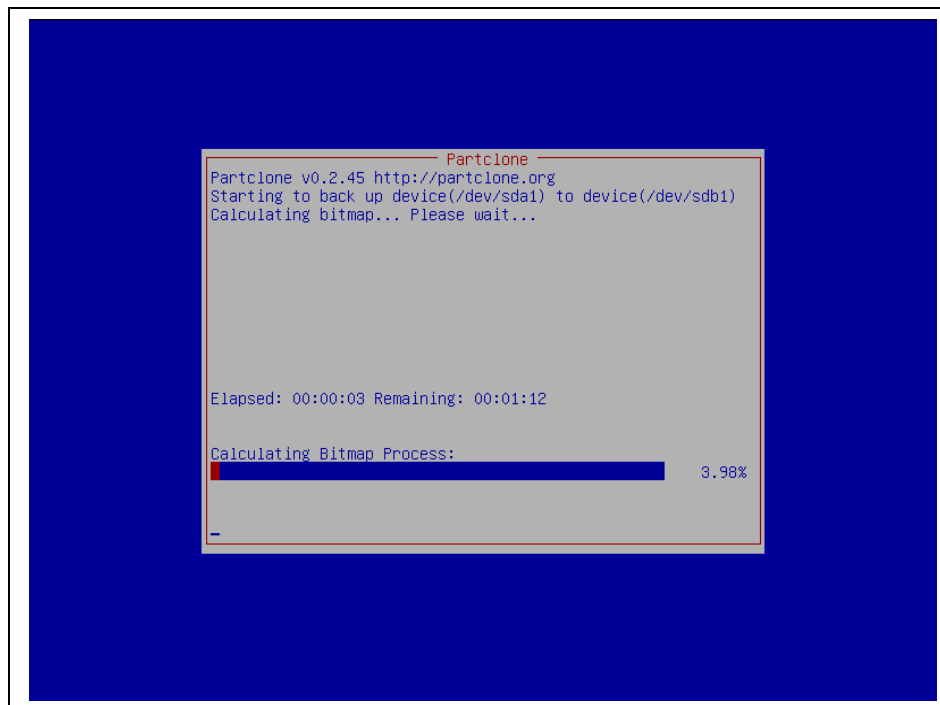
/dev/sdb2    292334805 312576704   20241900    7  HPFS/NTFS/exFAT
/dev/sdb3          0         -             0    0  Empty
/dev/sdb4          0         -             0    0  Empty
Successfully wrote the new partition table

Re-reading the partition table ...
[ 401.203002] sd 1:0:1:0: [sdb] Cache data unavailable
[ 401.203436] sd 1:0:1:0: [sdb] Assuming drive cache: write through
[ 401.203999] sdb: sdb1 sdb2

If you created or changed a DOS partition, /dev/foo7, say, then use dd(1)
to zero the first 512 bytes: dd if=/dev/zero of=/dev/foo7 bs=512 count=1
(See fdisk(8).)
This is done by "fdisk --force -C 19476 -H 255 -S 63 /dev/sdb < /tmp/ocs_onthefly_local.KBjdFM/tgt_
pt.sf"
Informing the OS that partition table has changed...
[ 401.279799] sd 1:0:1:0: [sdb] Cache data unavailable
[ 401.280630] sd 1:0:1:0: [sdb] Assuming drive cache: write through
[ 401.281165] sdb: sdb1 sdb2
Checking the integrity of partition table in the disk /dev/sdb...
done!
*****
The first partition of disk /dev/sdb starts at 63.
Restoring the hidden data between MBR (1st sector, i.e. 512 bytes) and 1st partition, which might be
useful for some recovery tool, by:
dd if=/tmp/ocs_onthefly_local.KBjdFM/tgt-hidden-data.img of=/dev/sdb seek=1 bs=512 count=62
62+0 records in
62+0 records out
31744 bytes (32 kB) copied, 0.00197847 s, 16.0 MB/s
*****
Do you want to clone the boot loader (executable code area, the first 446 bytes) to: sdb ?
[Y/n] y
Cloning the boot loader (executable code area) from "sda" to "sdb"...
*****
Now we will start to clone data to the target machine...
Are you sure you want to continue? ? (y/n)

```

One last check to make sure we really want to do this. Press 'y' then 'Enter' to continue.



The cloning process will start and may take some considerable time.

```

New volume size   : 10363851264 bytes (10364 MB)
Nothing to do: NTFS volume size is already OK.
*****
Creating the swap partition if exists...
*****
Trying to remove udev hardware record in the restored OS...
The specific destination disk is: sdb
Trying to remove udev persistent files. Searching in devices: sdb1 sdb2...
Skip /dev/sdb1 (ntfs).
Skip /dev/sdb2 (ntfs).
done!
*****
Run grub install on disk sdb...
The grub directory is NOT found. Maybe it does not exist (so other boot manager exists) or the file
system is not supported in the kernel. Skip running grub-install.
*****
Try to run partclone.ntfsfixboot for NTFS boot partition if it exists. Scanning partition(s): sdb1
sdb2...
Found NTFS boot partition among the restored partition(s): /dev/sdb1
Head and sector no. of /dev/sdb from EDD: 255, 63.
The start sector of NTFS partition /dev/sdb1: 63
Adjust filesystem geometry for the NTFS partition: /dev/sdb1
Running: partclone.ntfsfixboot -w -h 255 -t 63 -s 63 /dev/sdb1
ntfsfixboot version 1.0
done!
*****
If you want to use Clonezilla again:
(1) Stay in this console (console 1), enter command line prompt
(2) Run command "exit" or "logout"
*****
When everything is done, remember to use 'poweroff', 'reboot' or follow the menu to do a normal powe
roff/reboot procedure. Otherwise if the boot media you are using is a writable device (such as USB f
lash drive), and it's mounted, poweroff/reboot in abnormal procedure might make it FAIL to boot next
time!
*****
Press "Enter" to continue...

```

When the cloning process has completed, press 'Enter' to continue.

```

Trying to remove udev persistent files. Searching in devices: sdb1 sdb2...
Skip /dev/sdb1 (ntfs).
Skip /dev/sdb2 (ntfs).
done!
*****
Run grub install on disk sdb...
The grub directory is NOT found. Maybe it does not exist (so other boot manager exists) or the file
system is not supported in the kernel. Skip running grub-install.
*****
Try to run partclone.ntfsfixboot for NTFS boot partition if it exists. Scanning partition(s): sdb1
sdb2...
Found NTFS boot partition among the restored partition(s): /dev/sdb1
Head and sector no. of /dev/sdb from EDD: 255, 63.
The start sector of NTFS partition /dev/sdb1: 63
Adjust filesystem geometry for the NTFS partition: /dev/sdb1
Running: partclone.ntfsfixboot -w -h 255 -t 63 -s 63 /dev/sdb1
ntfsfixboot version 1.0
done!
*****
If you want to use Clonezilla again:
(1) Stay in this console (console 1), enter command line prompt
(2) Run command "exit" or "logout"
*****
When everything is done, remember to use 'poweroff', 'reboot' or follow the menu to do a normal powe
roff/reboot procedure. Otherwise if the boot media you are using is a writable device (such as USB f
lash drive), and it's mounted, poweroff/reboot in abnormal procedure might make it FAIL to boot next
time!
*****
Press "Enter" to continue...
"ocs-live-general" is finished.
Now you can choose to:
(0) Poweroff
(1) Reboot
(2) Enter command line prompt
(3) Start over
[0]


```


We can now select option '(0) Poweroff' to shut down the virtual system.

```

If you want to use Clonezilla again:
(1) Stay in this console (console 1), enter command line prompt
(2) Run command "exit" or "logout"
*****
When everything is done, remember to use 'poweroff', 'reboot' or follow the menu to do a normal poweroff/reboot procedure. Otherwise if the boot media you are using is a writable device (such as USB flash drive), and it's mounted, poweroff/reboot in abnormal procedure might make it FAIL to boot next time!
*****
Press 'Enter' to continue...
'ocs-live-general' is finished.
Now you can choose to:
(0) Poweroff
(1) Reboot
(2) Enter command line prompt
(3) Start over
[2] 0
INIT: Switching to runlevel: 0
INIT: Sending processes the TERM signal
Using makefile-style concurrent boot in runlevel 0.
Stopping mouse interface server: gpm.
Unmounting iscsi-backed filesystems: Unmounting all devices marked _netdev.
Stopping kernel log daemon....
Stopping system log daemon....
Asking all remaining processes to terminate...done.
All processes ended within 1 seconds...done.
rpcbind: rpcbind terminating on signal. Restart with "rpcbind -w"
Stopping rpcbind daemon....
Deconfiguring network interfaces...done.
Stopping NFS common utilities: idmapd statd.
Unmounting temporary filesystems...done.
Deactivating swap...done.
Stopping remaining crypto disks...done.
Stopping early crypto disks...done.
live-boot is resyncing snapshots and caching reboot files...
Please remove the disc, close the tray (if any) and press ENTER to continue:










```

 **Power on this virtual machine**

 **Edit virtual machine settings**

---

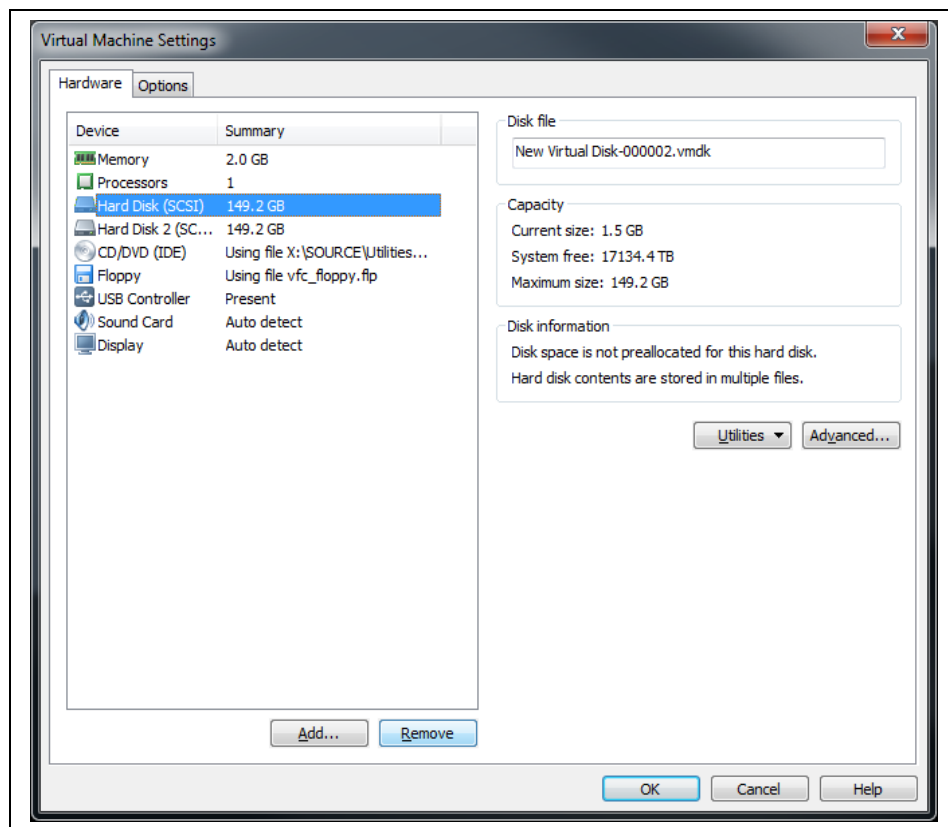
**▼ Devices**

 <b>Memory</b>	2.0 GB
 <b>Processors</b>	1
 <b>Hard Disk (SCSI)</b>	149.2 GB
 <b>Hard Disk 2 (SCSI)</b>	149.2 GB
 <b>CD/DVD (IDE)</b>	Using file X:\SO...
 <b>Floppy</b>	Using file vfc_flo...
 <b>USB Controller</b>	Present
 <b>Sound Card</b>	Auto detect
 <b>Display</b>	Auto detect

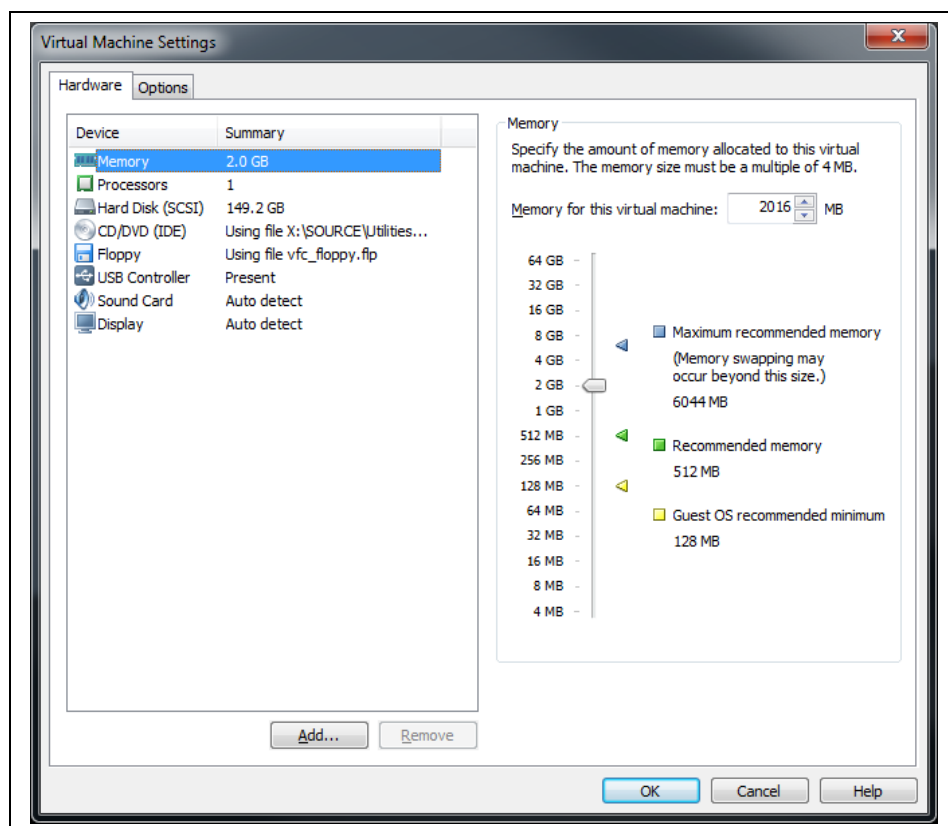
---

**▼ Description**

VM generated by VFC 2.11.11.11  
 from physical disk : \\.\PhysicalDrive11

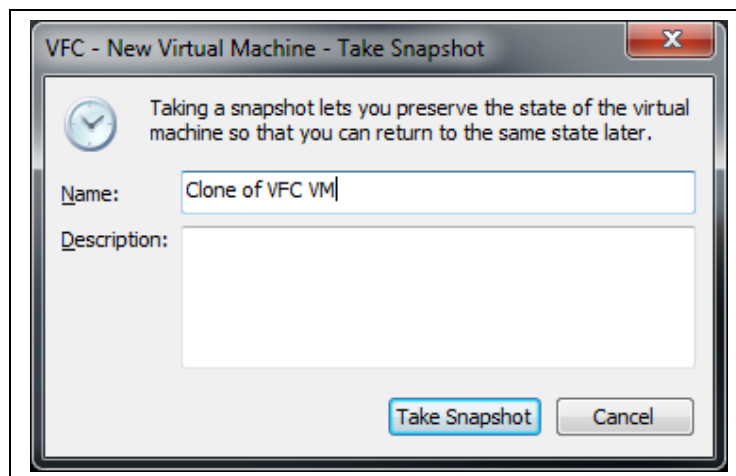
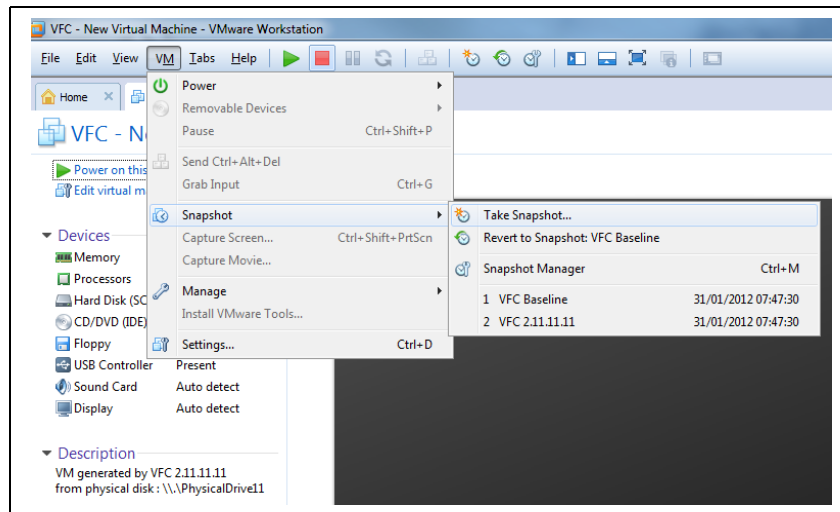


Use Edit virtual machine settings, select the original hard drive and use the 'Remove' button to remove this disk.






















You now need to take a snapshot of the system so that the initial state can be preserved if required.

If using VMware Workstation, simply use the menu option 'VM->Snapshot->Take snapshot' to create the snapshot of the system. This can be used at a later stage (via workstation) to revert the machine back to this initial state, if required.



NB The snapshot feature is not available in VMware Player.

You can now copy the entire folder containing your cloned VFC VM to a suitable medium for transfer to the client.

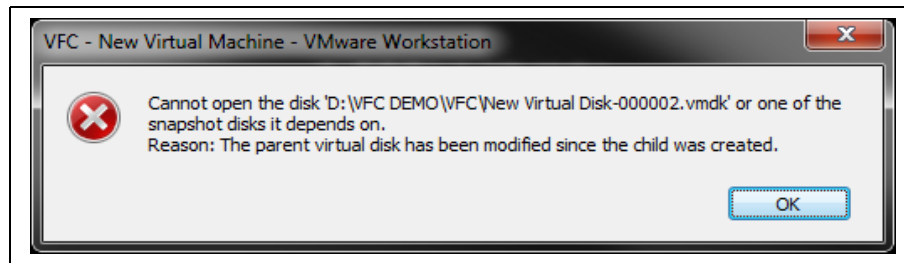
Name	Size
 New Virtual Machine.vmx.lock	
 vfc_floppy.flp	1,440 KB
 New Virtual Machine.VFC2.log	2 KB
 vmware.log	108 KB
 vmware-0.log	180 KB
 vmware-1.log	106 KB
 vmware-2.log	105 KB
 Clone of New Virtual Machine.vmdk	29,282,240 KB
 Clone of New Virtual Machine-000001.vmdk	19,200 KB
 New Virtual Disk.vmdk	1 KB
 New Virtual Disk-000001.vmdk	58,880 KB
 New Virtual Disk-000002.vmdk	65,600 KB
 New Virtual Machine.vmsd	2 KB
 New Virtual Machine.vmx	1 KB
 Microsoft Windows XP.nvram	9 KB
 New Virtual Machine.vmx	3 KB
 New Virtual Machine-Snapshot1.vmsn	11 KB
 New Virtual Machine-Snapshot2.vmsn	11 KB
 New Virtual Machine-Snapshot3.vmsn	20 KB

Note that the 'Clone of New Virtual Machine.vmdk' only occupies 27.9GB of disk space, even though it is capable of increasing in size to the full 149.2GB capacity.

The 'Clone of New Virtual Machine-000001.vmdk' is the snapshot file that was created to preserve the state of the original cloned disk. Subsequent disk writes will be 'captured' in this snapshot file and can be discarded (if desired) by using the 'Revert to Snapshot' function of VMware Workstation.

## Known Issues & Troubleshooting

### *Cannot open the disk*

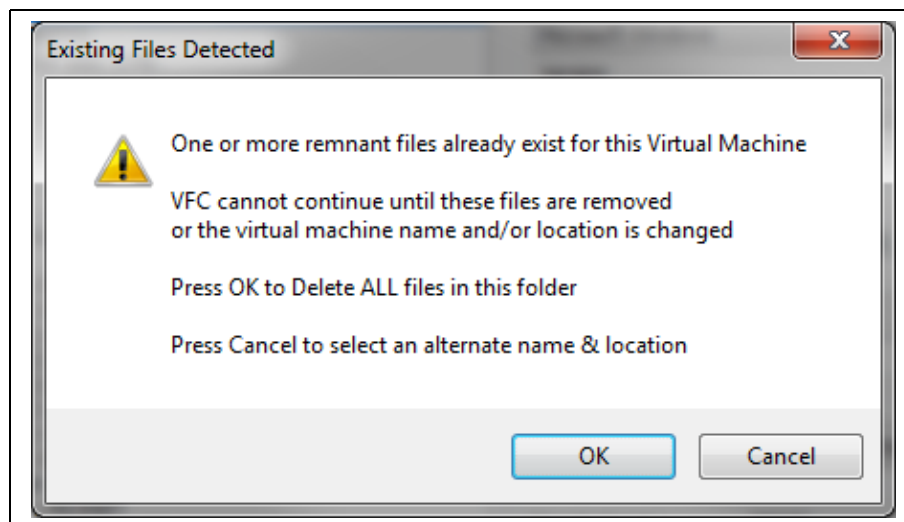


There may be occasions when the VFC generation appears to function seamlessly yet a message similar to that displayed above is encountered when starting the machine.

This issue is caused by an inconsistency in the time stamps of the generated virtual disk cache files and has been found to occur most often when Windows Explorer is open during the generation process. This is believed to cause an issue with cleanly dismounting the disk cache via vmware-mount.

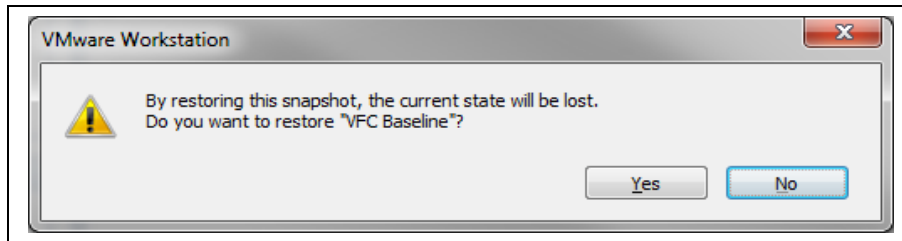
There are several methods to resolve this issue if it is encountered.

- (i) Regenerate the virtual machine in the same folder, discarding the existing files.



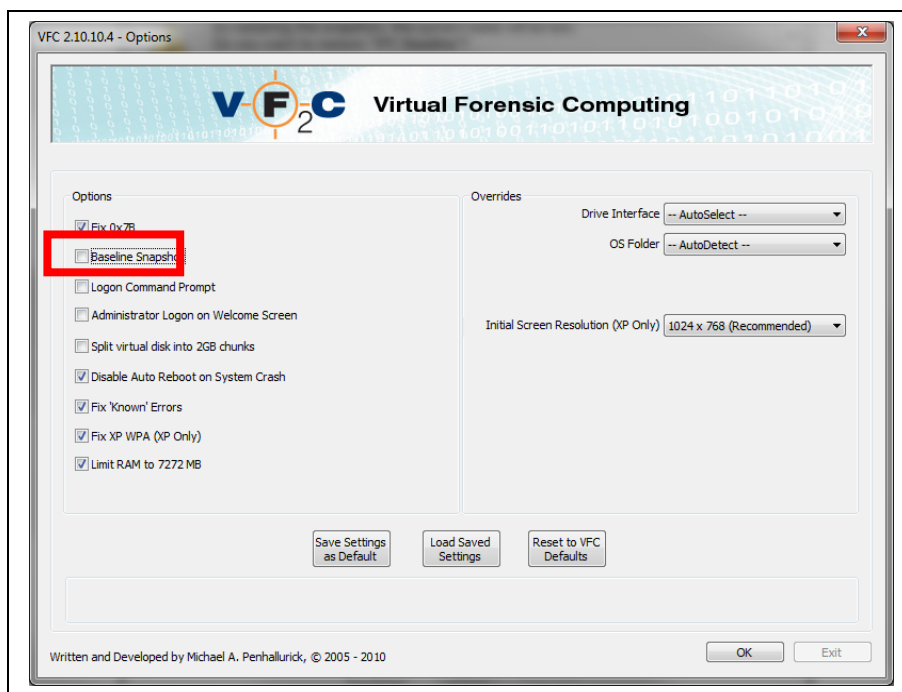


- (ii) Revert to snapshot (if using Workstation) – this will flush the latest disk cache and reset the problem time stamps.



*(If reverting to snapshot, do the process twice as otherwise the snapshot numbering sequence may latterly fall out of sync.)*

- (iii) Disable the baseline snapshot option via the Options button on the main dialog screen prior to generating the VFC VM.



*Host System is Windows 7 on a Boot Camp Mac Pro*

It has been identified that when running Windows 7 on a Boot Camp Apple Mac Pro (and potentially other Mac hardware), VFC does not function as expected during the analysis and generate VM procedures.

It is believed that the installation of the Apple Boot Camp drivers causes an issue with VFC whereby the mounted disk caches (generated as part of the analysis and generation stages of the VFC virtualisation process) fail to be read correctly.

This failure to read the mounted cache partition leads to errors detecting the operating system and injecting the requisite patch code into the subject registry.

**The current resolution is to remove the Boot Camp drivers, whereby it has been found that the VFC will function as expected.**

Investigation and development continues in order to attempt to make VFC fully compatible with the a Windows installation which incorporates the Apple Mac Boot Camp drivers.

## *Could Not Unload Registry*

There is an intermittent permissions issue (especially with Vista SP1) whereby a subject registry cannot be unloaded from the host system during generation. This will cause the current session to fail and may cause subsequent sessions to also fail. In these instances it is necessary to exit VFC and manually unload any remnant hives.

*The resultant VFC VM may not function correctly thereafter but once generated can be re-patched by utilising the Restore Points methodology described above.*

VFC 2.11.11.11 includes a program initialisation check to remove any remnant hive data from such an occurrence. Simply exit and restart the VFC to remove any remnant hives. Older versions of VFC require the remnant hives to be unloaded manually.

### **CAUTION:**

**If you make a mistake when you edit the registry, your system might become unstable or unusable. Proceed with caution.**

To manually unload any remnant hives which VFC cannot automatically unload, first make sure that the VFC application is closed.

Next, start REGEDIT and expand HKEY\_LOCAL\_MACHINE.

If there are entries for NEWSYSTEM, NEWSOFTWARE or NEWDEFAULT, these are remnant hives that have not been cleanly unloaded by VFC.

Select the remnant hive and use the menu 'File', 'Unload Hive' to remove the remnant hive from the system. If the hive still cannot be unloaded, you may need to first restart the system to flush any system locks that are still present. Once all remnant hives have been removed, exit REGEDIT, dismount any mounted images and restart the system.

To use the Restore Points method on the failed VFC VM, first make sure that any required disk image files have been mounted as previous and then use the 'Open Existing' option from the VFC main dialog to ensure that the PHYSICALDRIVE number allocation is consistent and matches that which VFC has recorded against the VFC VM.

Once 'Open Existing' has verified that the VFC VM is ready to launch, try to 'Launch' the VFC VM. This may result in a 0x7B BSOD. If so use the Restore Points methodology to try to re-inject necessary parameters into the VFC VM.

If the machine cannot be launched with a 'Cannot open the disk' error, follow the steps as above to resolve the snapshot time-stamp issue.

## **Frequently Asked Questions**

### **Which Disk Formats are supported by VFC?**

VFC continues to develop and currently supports:-

- Forensic image files mounted using Mount Image Pro v2, v3 & v4
- Forensic image files mounted using AccessData FTK Imager 3
- Forensic image files disk emulated using Guidance Software Encase PDE (Physical Disk Emulator)
- (write blocked) original physical disks (IDE, SATA, USB, IEEE1394)
- Unix style uncompressed 'dd' images and,
- Vagon format uncompressed 'img' images.

### **Which Systems can be booted using VFC?**

VFC has been used to successfully boot:

- Windows 3.1
- Windows 95
- Windows 98
- Windows ME
- Windows NT
- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008
- Linux (experimental)
- MAC OS X (10.5 and above) (experimental)

### **What do I need to run VFC?**

VFC utilises the freely available VMware Player and VMware Disk Mount Utility, in conjunction with Mount Image Pro to mount forensic images files. VFC requires Windows XP or higher and also requires that you be logged in with Administrator level privileges.

### **Do I need to have Mount Image Pro or Encase?**

No. VFC is wholly capable of using physical disks or 'dd' images.

Mount Image Pro is only required if you have forensic evidence files in the Expert Witness Format which you would like to access outside of any forensic suite.

Encase is only required if you wish to utilise the Encase PDE in order to emulate a physical disk.

## **How Do I Use VFC?**

VFC is as easy to use as 1-2-3:

1. Mount the evidence file (or attach the [write-blocked] physical disk)
2. Select the disk (or dd image) and the relevant partition
3. Generate the machine and use the Launch feature to start it in VMware.

## **What limitations does VFC have?**

VFC will successfully boot 95% of Windows based disks / images it is presented with. VFC cannot dynamically fix machines that are 'broken' and unable to be booted in the original machine. Similarly, VFC cannot bypass software protection that is linked / licensed to the original hardware.

## **Will booting an image using VFC alter the original evidence?**

VFC dynamically creates a custom disk cache and directs all subsequent reads and writes 'through' this disk cache. The original evidence is only ever 'read' and cannot be directly written to. Additionally, mounted or emulated forensic image files are opened read-only by default, as are 'dd' and 'img' disk image files.

**NB** *If you are using physical disks, it is imperative that you use a hardware write-blocking device to connect this disk to your own system, otherwise your host system will almost certainly try to write to the physical disk and this will change the evidence.*

## **Does VFC support partition only images?**

Yes. Partition image support is included. Development continues to implement multi-partition image support.

## **Does VFC support multi-boot systems?**

Full multi-boot system support is under development.

## **I've used VFC but still get a BSOD halfway through the boot sequence!**

It may be necessary to boot into safe mode and disable services specific to the original hardware, such as:

- NVidia or ATI graphic drivers,
- custom audio drivers or
- OEM specific utilities.

## **Do I need to install the drivers for the New Detected Hardware?**

It is not absolutely necessary to install these drivers, however the virtual machine may not function properly without them and you may find that the CD, mouse or floppy disk (for example) do not function at all. It is recommended that you let the VM detect and install the necessary files.

## **How can I improve the performance of the New Virtual Machine?**

If you are using either VMware Workstation or VMware Server or VMware Player 3 or above, you can install the VMware Tools Package to improve the performance of your virtual machine. This option is not directly available with the standalone VMware Player 2 or earlier.

## **Can I access the Internet from the New Virtual Machine?**

VFC is designed to be a forensic application and does not add any network support to the New Virtual Machine to ensure it remains isolated from the 'real' world. It is possible to add network support and hence connect to other networks (including the Internet), but this is not recommended. Adding Network support is currently a manual process undertaken at the discretion of the user.

## **Can I transfer data between the New Virtual Machine and my own System?**

You can use virtual (or real) floppy disks, USB devices and you can even connect a physical data disk as a raw device and write directly to that disk. You can also use CD/DVD media (or ISO files) to read data into the New Virtual Machine.

If VMware Tools have been installed, you can drag and drop from the VFC virtual machine to your own Host machine and vice versa.

**NB** Not all of these methods are readily available with the standalone VMware Player.

## **Why does the New Virtual Machine need to be activated?**

Windows XP and above may require activation due to the number of hardware changes that are inevitable from changing between a physical and a virtual environment. Not all machines can successfully be activated but all machines should be able to be accessed in 'Safe Mode' and this will enable at least a partial interaction with the original desktop.

## **Can I create additional Snapshots?**

Yes, VFC allows the VM to create multiple snapshots. Snapshot creation is dependant upon the version of VMware being utilised.

## **What does VFC actually do?**

VFC creates a disk cache that is used by VMware to intercept any changes to the underlying original disk, whether this is a physical device, mounted forensic image or a full bit-for-bit image file.

VFC makes the minimum necessary modifications via the disk cache in order to ensure that it can successfully boot in a virtual environment.

The whole ethos behind VFC is to keep the underlying image as close as possible to the original and yet still make it function in VMware. In situ upgrades, which are advocated as one method of achieving the same goal, were deemed too intrusive of the 'forensic' process.

## **The Creator of VFC**

Michael A. Penhallurick holds a Master of Science Degree in Forensic Computing from the Royal Military College of Science / Cranfield University and was a regular visiting lecturer at that establishment between 2002 and 2005. He has also been involved in the development of training packages with the National Specialist Law Enforcement Centre Hi Tech Crime Training Team.



Michael joined MD5 Limited in November 2006 having previously served as a Police Officer with the South Yorkshire Police for almost 13 years, the last four years of which were as Computer Forensic Manager for their Hi-Tech Crime Unit. He also undertook a year as Computer Forensics Manager in a corporate environment for The Risk Advisory Group based in the centre of London.

In both roles he was responsible for undertaking and overseeing major criminal investigations for a variety of criminal activities ranging from indecency through to fraud and murder. He was also responsible for ensuring the smooth day-to-day running of the unit including staff development and identification of training needs, as well as liaison with external agencies such as the Crown Prosecution Service, the Probation Service and the Courts and regular client conferences.

Michael has been involved in computing in general since 1986 and prior to joining the Police Service he lived and worked in Dubai, United Arab Emirates, as a freelance computer systems consultant for both small and large businesses including financial advisors, several oil companies, an aerial survey company, the Dubai Ports Authority and the Government of Dubai Water Department.

Michael has been involved in Forensic Computing since 1997 and has had extensive training and first hand use of the Vognon, Encase, AccessData and iLook suites of forensic tools.



## Download Links

VMware Workstation 8.0.2

[http://downloads.vmware.com/d/info/desktop\\_end\\_user\\_computing/vmware\\_workstation/8\\_0](http://downloads.vmware.com/d/info/desktop_end_user_computing/vmware_workstation/8_0)

VMware Player 4.0.2

[http://downloads.vmware.com/d/info/desktop\\_end\\_user\\_computing/vmware\\_player/4\\_0](http://downloads.vmware.com/d/info/desktop_end_user_computing/vmware_player/4_0)

VMware VDDK

<http://www.vmware.com/support/developer/vddk/>

Mount Image Pro

<http://www.mountimage.com/>

VFC

<http://www.md5.uk.com/products/vfc2/download-vfc>